Vulnerability Assessment Report
For
LIVMOR Web Portal

January 2020

Document History

Ver. Rel. No.	Release Date	Prepared. By Prepared. Dt.	Reviewed By	Approved By	Remarks/Revision Details
1.0	1/22/2020	Abhijeet Kumar	Sathya Subbiah	Sathya Subbiah Vibin PV	WebPortal Assessment Report

Contents

1. Overview of the project

This assessment was aimed to perform Vulnerability Assessment and Penetration Testing (VAPT) on LIVMOR Web Portal which has the URL - https://heartview001.livmor.com/HeartView. LIVMOR's wearable platform aims to record key health parameters of the patient and showcase it to both the doctor as well as the patient. The data is processed in ways to help them monitor and maintain key parameters under prescribed levels.

Objective of the security assessment:

L&T Technology Services (LTTS) has conducted Web Application Security Assessment of LIVMOR Web Portal. The purpose of the assessment is to evaluate the security of the application against common vulnerabilities with the primary reference being OWASP top 10 vulnerabilities lists.

Approach

The following approach was taken to make sure the target site is assessed against OWASP Top 10 Vulnerabilities from all possible security perspectives:

- Manual Penetration Testing Techniques.

Testing Environment Details

Target site URL	https://heartview001.livmor.com/HeartView/
Browser	Chrome, IE, Mozilla
Proxy / Interceptors	BURP, ZAP, Wireshark

Key Security Policies

OWASP top 10 listed vulnerabilities were used as a reference framework. The following key security aspects were checked:

1. Input Data validation.
2. Error Handling.
3. Information disclosure.
4. Authentication Mechanism.
5. Session and status information.
6. Malicious data validation.
7. Client side security.
8. Server side security.

The following attack vectors were used:

1. Account Takeover
2. Insecure HTTP Methods Enabled
3. File Upload Checks at Server
4. Session Invalidation Recover Password
5. XSS
6. Unencrypted Transport
7. Directory Traversal
8. No Account Lockout
9. Concurrent Session Remain Active
10. Session Replay
11. Privilege Escalation
12. Cross site Request Forgery
13. Click Jacking
14. Server side Validation
15. Server side Password Complexity Check
16. Insecure Direct Object Reference
17. Server Banner Disclosure
18. Password Autocomplete in Browser
19. NOSQL Injection
20. Path Traversal
21. XML External Entity
22. Insecure Deserialization

2. Assessment explained in detail

Attack vectors enable the hackers to exploit the vulnerabilities in the system and thus compromise the security of the system. To assess the security of the LIVMOR web portal the following attack vectors are used

1. Account Takeover
2. Insecure HTTP Methods Enabled
3. File Upload Checks at Server
4. Session Invalidation Recover Password
5. XSS
6. Unencrypted Transport
7. Directory Traversal
8. No Account Lockout
9. Concurrent Session Remain Active
10. Session Replay
11. Privilege Escalation
12. Cross site Request Forgery
13. Click Jacking
14. Server side Validation
15. Server side Password Complexity Check
16. Insecure Direct Object Reference
17. Server Banner Disclosure
18. Password Autocomplete in Browser
19. NOSQL Injection
20. Path Traversal
21. XML External Entity
22. Insecure Deserialization

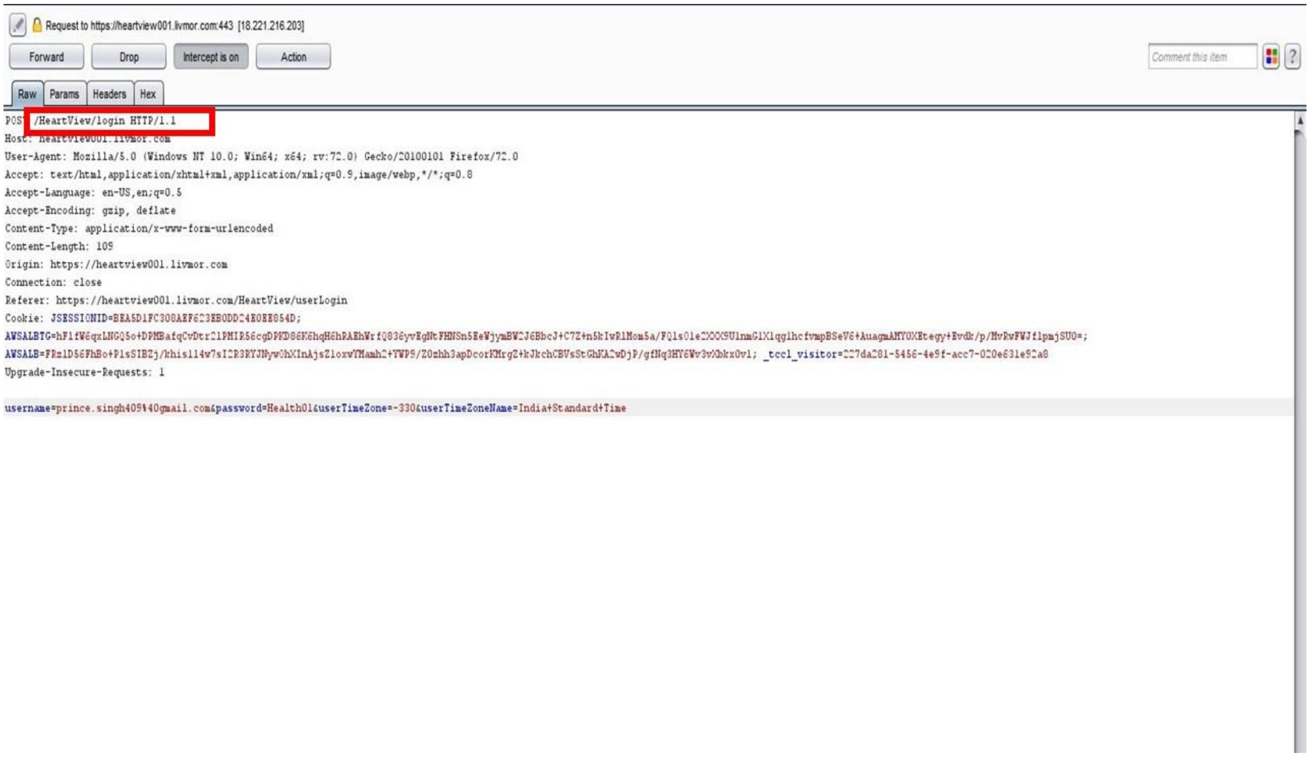
Vulnerabilities are found on performing the attack vectors Insecure HTTP Methods Enabled, Concurrent Session Remain Active, Session Replay, Privilege Escalation, Click-Jacking, Password Autocomplete in Browser. No vulnerability discovered during the execution of the remaining attack vectors.

2.1. Evidences for Unsuccessful Exploit Attempts

2.1.1 Session Invalidation Recover Password

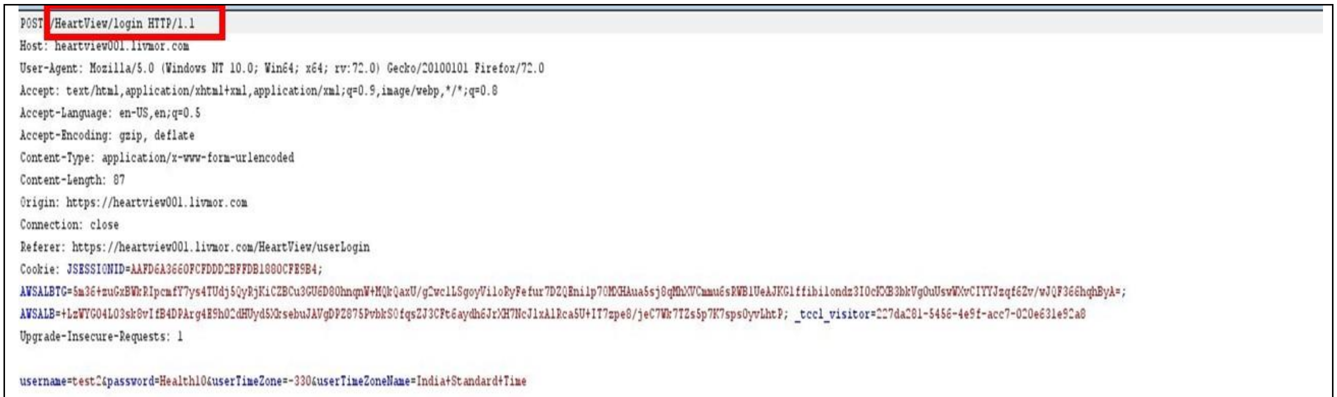
Description: Security misconfiguration can happen at any level of an application stack, including platform, web server, application server, database, frameworks, or custom code. These flaws frequently give attackers unauthorized access to some user data or functionality. Anonymous external attackers as well as authorized users may attempt to compromise the system/users of the system to disguise their actions.

Evidence



```
POST /HeartView/login HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 109
Origin: https://heartview001.livmor.com
Connection: close
Referer: https://heartview001.livmor.com/HeartView/userLogin
Cookie: JSESSIONID=BEA5D1FC308AEF623EB0DD24E0EE854D;
AWSALBTG=hF1fW6qxLNGQ5o+DPMBafqCvDtr21PMIR56cgDPKD86K6hqH6hRAEhWrfQ836yvEgNtFHNSn5EeWjymBW2J6BbcJ+C7Z+n5kIwRlMom5a/FQ1s01e2XXX9UlnmG1X1qglhcfvmpBSeV6+AuagmAMY0XEtegy+Evdk/p/MvRwFWJflpmjSU0=;
AWSALB=FRzlD56FhBo+PlsSIBZj/khisl14w7sI2R3RYJNyw0hXInAjsZloxwYMamh2+YWP9/Z0zhh3apDcorKMrgZ+kJkchCBVsStGhKA2wDjP/gfNq3HY6Wv3vXbkx0vl; _tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8
Upgrade-Insecure-Requests: 1

username=prince.singh409%40gmail.com&password=Health01&userTimeZone=-330&userTimeZoneName=India+Standard+Time
```

User Id is not being sent through URL so we are not able to tamper it (Physician's Account)



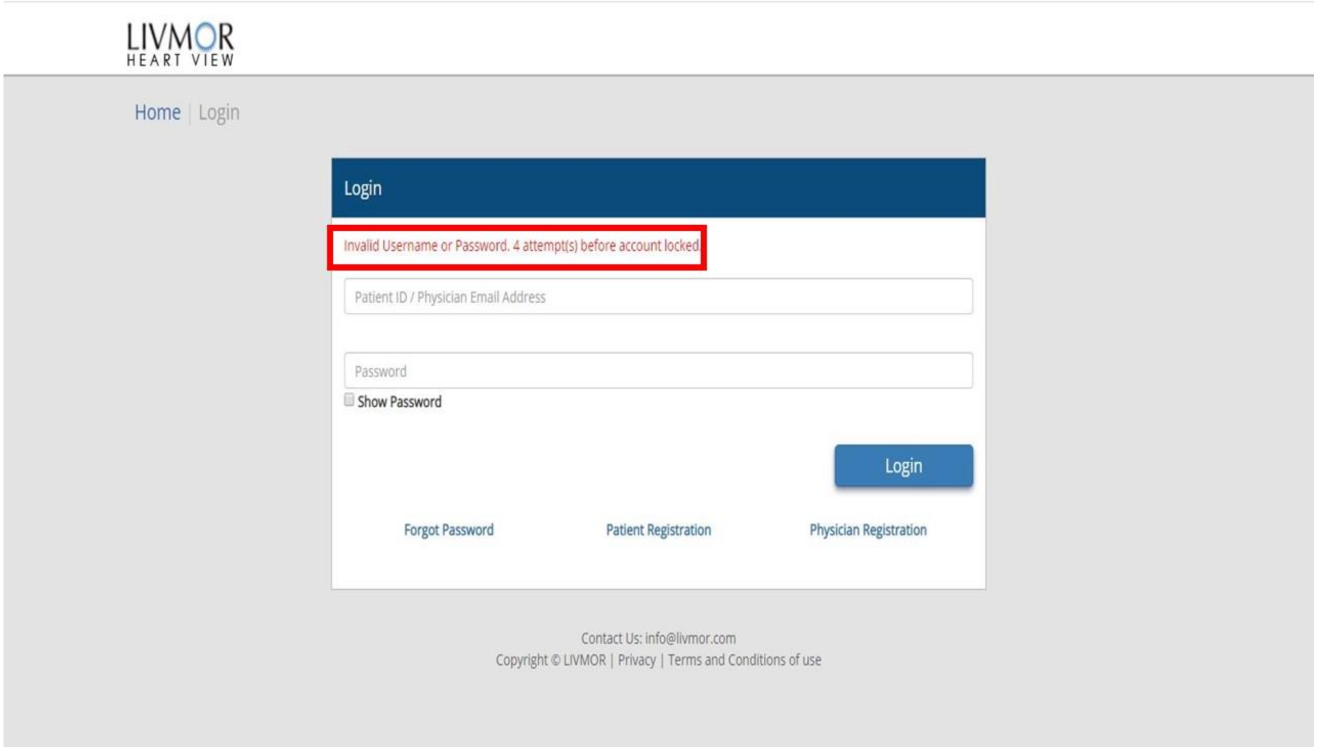
```
POST /HeartView/login HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
Origin: https://heartview001.livmor.com
Connection: close
Referer: https://heartview001.livmor.com/HeartView/userLogin
Cookie: JSESSIONID=AAFD6A3660FCFDDD2BFFDB1880CFE9B4;
AWSALBTG=5m36+zuGxBWkRIpcmfY7ys4TUdj5QyRjKiCZBCu3GU6D80hnqnW+MQkQaxU/g2wclLSgoyViloRyFefur7DZQEnilp70MXHAua5sj8qMhXVCmmu6sRWB1UeAJKGlffibilondz3I0cKXB3bkVg0uUswWXvCIYYJzqf6Zv/wJQF366hqhByA=;
AWSALB=+LzWYG04L03sk8vIfB4DPArg4E9h02dHUyd5XrsebuJAVgDPZ875PvbkS0fqsZJ3CFt6aydh6JrXH7NcJ1xAlRca5U+IT7zpe8/jeC7Wk7TZs5p7K7sps0yvLhtP; _tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8
Upgrade-Insecure-Requests: 1

username=test2&password=Health10&userTimeZone=-330&userTimeZoneName=India+Standard+Time
```

User Id is not being sent through URL so we are not able to tamper it (Patient’s Account)

2.1.2 No Account Lockout (for patient)

Description: Account lockout mechanisms are used to mitigate brute force password guessing attacks. Accounts are typically locked after 3 to 5 unsuccessful login attempts and can only be unlocked after a predetermined period, via a self-service unlock mechanism, or intervention by an administrator.

Evidence



Invalid Username or Password. 4 attempt(s) before account locked

Contact Us: info@livmor.com

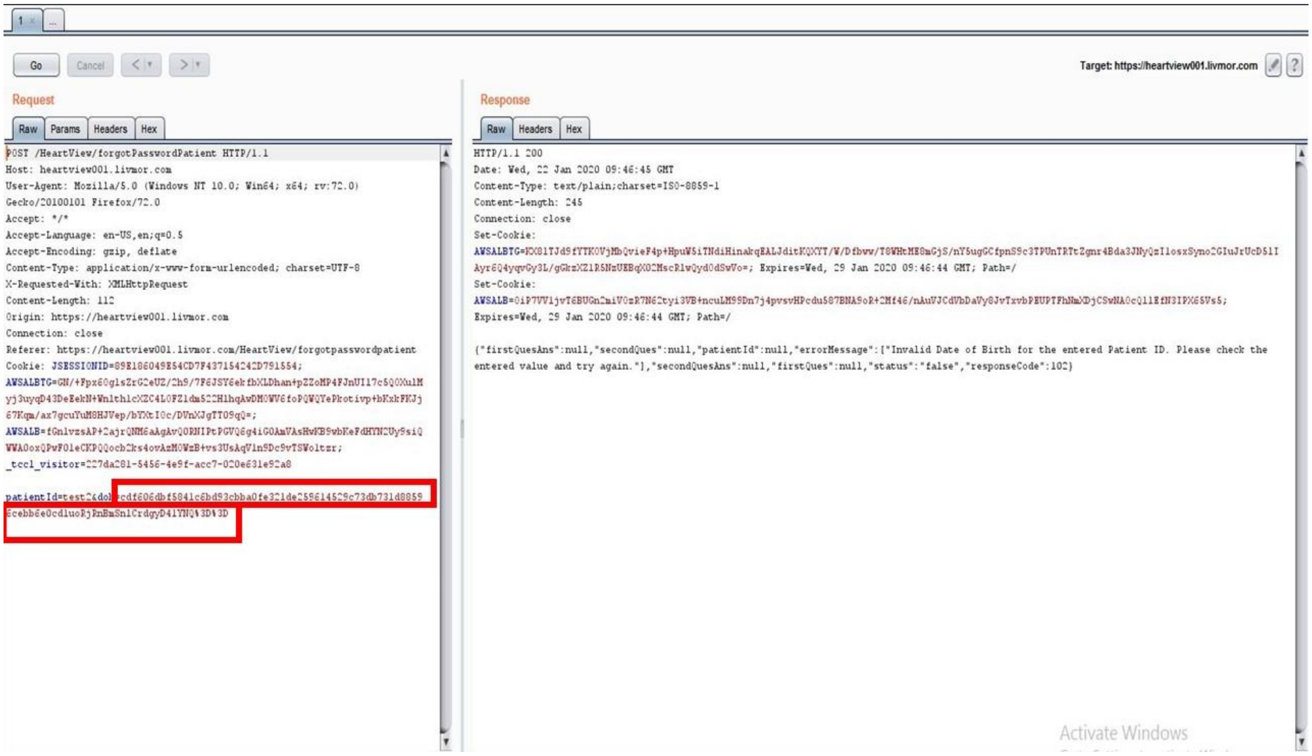
Copyright © LIVMOR | Privacy | Terms and Conditions of use

Login attempts are implemented successfully.

2.1.3 Account Takeover

Description: Developers frequently build custom authentication and session management schemes, but building these correctly might be difficult. As a result, these custom schemes might have flaws in areas such as logout, password management, timeouts, remember me, secret question, account update, etc. Users with their own accounts, may attempt to steal accounts from others. Also consider insiders wanting to disguise their actions. Attacker uses leaks or flaws in the authentication or session management functions (e.g., exposed accounts, passwords, session IDs) to impersonate users.

Evidence



```
POST /HeartView/forgotPasswordPatient HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 112
Origin: https://heartview001.livmor.com
Connection: close
Referer: https://heartview001.livmor.com/HeartView/forgotpasswordpatient
Cookie: JSESSIONID=89E186049E54CD7F437154242D791554;
AWSALBTG=GN/+Fpx60glsZrG2eUZ/2h9/7F6JSY6ekfbXLDhan+pZZoMP4FJnUI17c5Q0XulM
yj3uyqD43DeEekN+Wnlthlc XZC4L0FZ1dm522HlhqAwDM0WV6foPQWQYePkotivp+bKxkFKJj
67Kqm/ax7gcuYuM8HJVep/bYXtI0c/DVnXJgTT09qQ=;
AWSALB=fGnlvzsAP+2ajrQNM6aAgAvQ0RNIPtPGVQ6g4iG0AmVAsHwKB9wbKeFdHYN2Uy9siQ
WWA0oxQPwF0leCKPQQocb2ks4ovAzM0WzB+vs3UsAqVln9Dc9vTSWoltzr;
_tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8

patientId=test2&dob=cdf606dbf5841c6bd93cbba0fe321de259614529c73db731d8859
6cebb6e0cdluoRjRnBmSnlCrdgyD41YNQ%3D%3D
```

```
HTTP/1.1 200
Date: Wed, 22 Jan 2020 09:46:45 GMT
Content-Type: text/plain;charset=ISO-8859-1
Content-Length: 245
Connection: close
Set-Cookie:
AWSALBTG=KX81TJd9fYTK0VjMbQvieF4p+HpuW5iTNdiHinakqEALJditKQXYT/W/Dfbww/T8WHtME8mGjS/nY5ugGCfpnS9c3TPUnTRTtZgnr4Bda3JNyQzIlosxSyno2GIuJrUcD51I
Ayr6Q4yqvGy3L/gGkzXZ1R5NzUEBqX02MscRlwQyd0dSwVo=; Expires=Wed, 29 Jan 2020 09:46:44 GMT; Path=/
Set-Cookie:
AWSALB=0iP7VV1jvT6BUGn2miV0zR7N62tyi3VB+ncuLM99Dn7j4pvsvHPcdu587BNA9oR+2Mf46/nAuVJCdVbDaVy8JvTxvbPEUPTFhNmXDjCSwNA0cQ11EfN3IPX65Vs5;
Expires=Wed, 29 Jan 2020 09:46:44 GMT; Path=/

{"firstQuesAns":null,"secondQues":null,"patientId":null,"errorMessage":["Invalid Date of Birth for the entered Patient ID. Please check the
entered value and try again."],"secondQuesAns":null,"firstQues":null,"status":"false","responseCode":102}
```

The DOB parameter is encoded and cannot be altered.

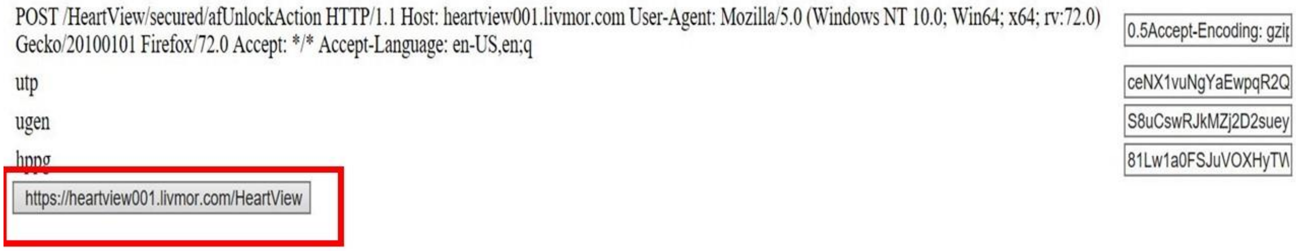
2.1.4 Cross Site Request Forgery

Description: Cross-site request forgery (CSRF) vulnerabilities arise when applications rely solely on HTTP cookies to identify the user interacting with the server by making requests. Browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. When a user who is logged in to the application visits the attacker's website, the user's browser issues the request, which includes the user's session or authentication cookie. The application relies solely on HTTP cookies.

Evidence

The generated POC for CSRF (Cross Site Request Forgery) is here. If it was vulnerable to CSRF attack, after clicking to submit request it should login to the existing page.

Request



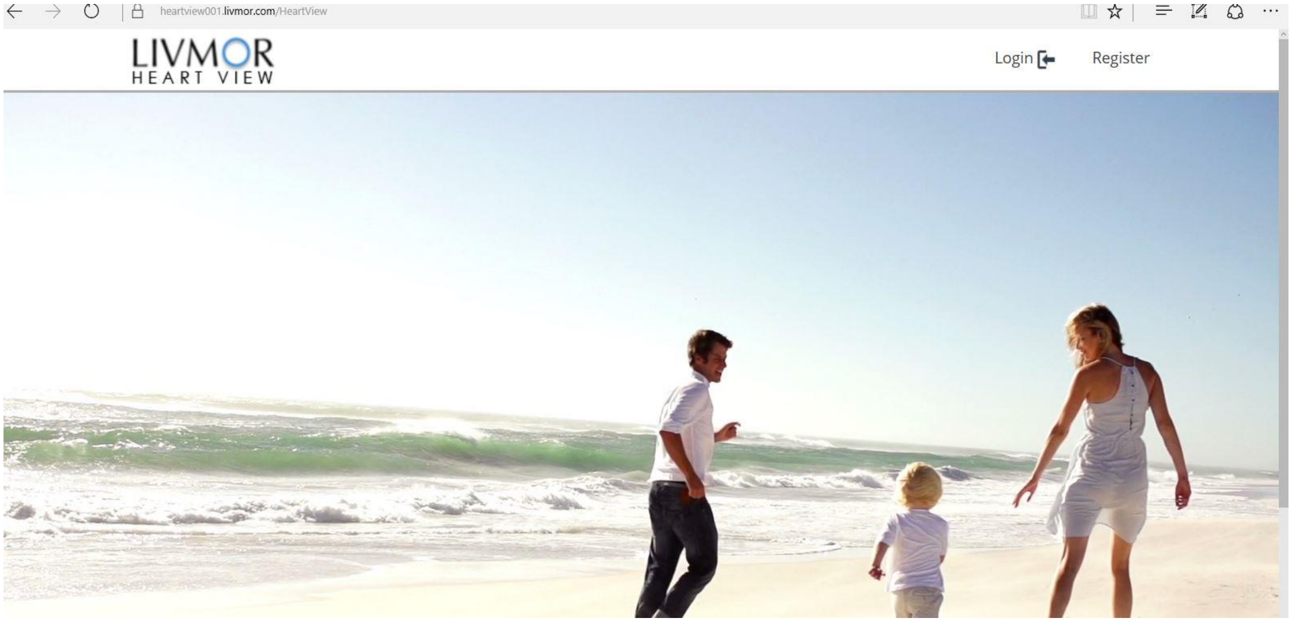
POST /HeartView/secured/afUnlockAction HTTP/1.1 Host: heartview001.livmor.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0 Accept: */* Accept-Language: en-US,en;q 0.5Accept-Encoding: gzi

utp ceNX1vuNgYaEwpqR2Q

ugen S8uCswRJkMZj2D2suey

hppg 81Lw1a0FSJuVOXHyTW

Response in Browser



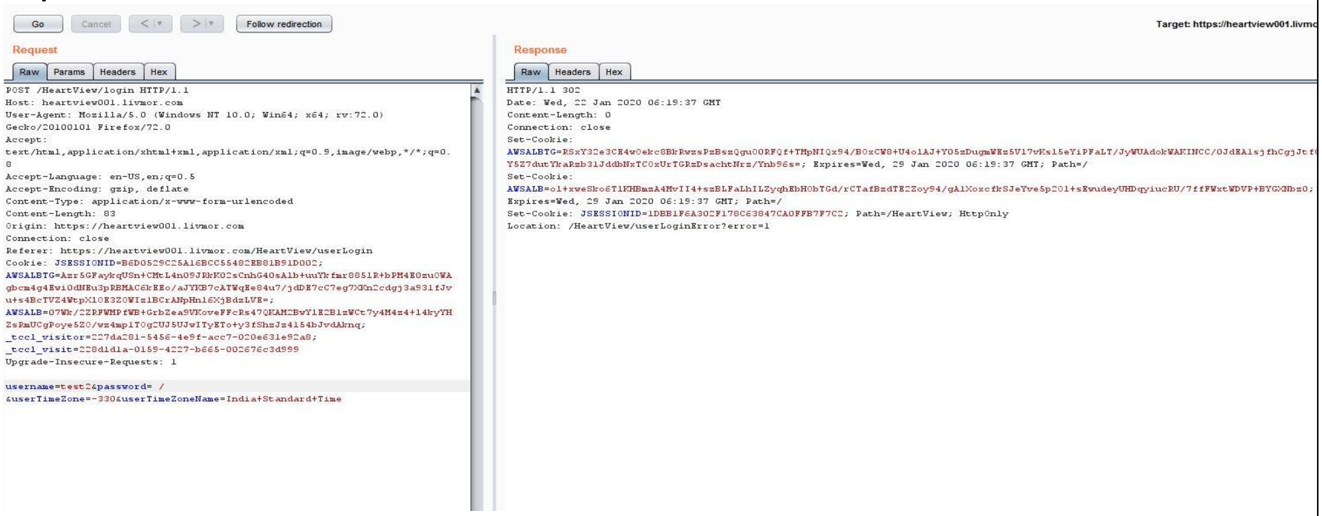
But it is not allowing the attacker to go inside the application. So, it is not vulnerable to CSRF attack.

2.1.5 Server Side Validation

Description: The mandatory fields check for the user registration function is only performed on client side but not on the server side, by tampering the parameters through intercepting the request can bypass the mandatory requirements and set NULL value. Users with penetration skills can bypass mandatory field requirements.

Evidence

Request

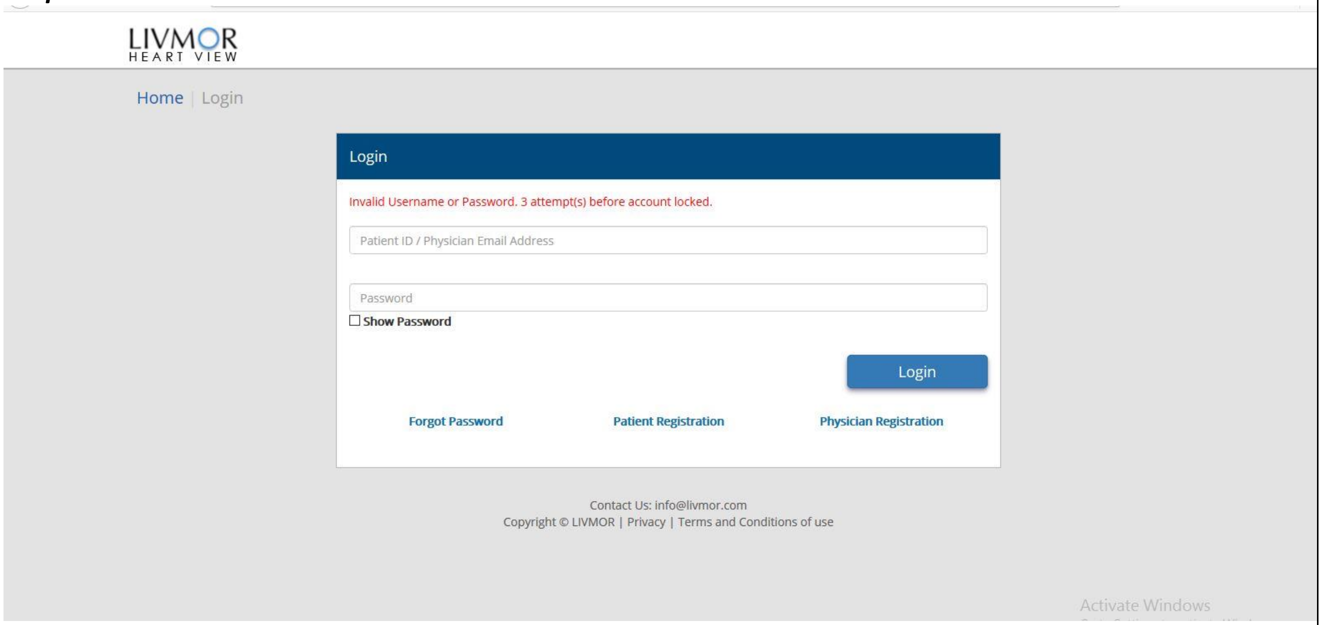


```
POST /HeartView/login HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
Origin: https://heartview001.livmor.com
Connection: close
Referer: https://heartview001.livmor.com/HeartView/userLogin
Cookie: JSESSIONID=B6D0529C25A16BCC55482EB81B91D002;
AWSALBTG=Azr5GFaykqUSn+CMtL4n09JRkK02sCnhG40sAlb+uuYkfmr8851R+bPM4E0zu0WA
gbcm4g4Ewi0dNEu3pRBMAC6kEEo/aJYKB7cATWqEe84u7/jdDE7cC7eg7XKn2cdgj3a931fJv
u+s4BcTVZ4WtpXl0E3Z0WIzlBCrANpHnl6XjBdzLVE=;
AWSALB=07Wk/2ZRFWMPfWB+GrbZea9VKoveFFcRs47QKAM2BwYlE2BlzWCt7y4M4z4+14kyYH
ZsRmUCgPoye5Z0/wz4mplT0g2UJ5UJwITyETo+y3fShzJz4154bJvdAknq;
_tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8;
_tccl_visit=228d1d1a-0159-4227-b665-002676c3d999
Upgrade-Insecure-Requests: 1

username=test2&password= /
&userTimeZone=-330&userTimeZoneName=India+Standard+Time
```

```
HTTP/1.1 302
Date: Wed, 22 Jan 2020 06:19:37 GMT
Content-Length: 0
Connection: close
Set-Cookie:
AWSALBTG=RSxY32e3CE4w0ekc8BkRwzsPzBszQgu0ORFQf+TMpNIQx94/B0xCW8+U4olAJ+Y05zDugmWEz5V17vKsl5eYiPFaLT/JyWUAdokWAKINCC/0JdEAlsjfhCgjJtf
Y5Z7dutYkaRzb31JddbNxTC0xUrTGRzDsachtNrz/Ynb96s=; Expires=Wed, 29 Jan 2020 06:19:37 GMT; Path=/
Set-Cookie:
AWSALB=ol+xweSko6T1KHBmzA4MvII4+szBLFaLhILZyqhEbH0bTGd/rCTafBzdTE2Zoy94/gAlXoxcfkSJeYve5p201+sEwudeyUHDqyiucRU/7ffFWxtWDVP+BYGXNbz0;
Expires=Wed, 29 Jan 2020 06:19:37 GMT; Path=/
Set-Cookie: JSESSIONID=1DBB1F6A302F178C63847CA0FFB7F7C2; Path=/HeartView; HttpOnly
Location: /HeartView/userLoginError?error=1
```

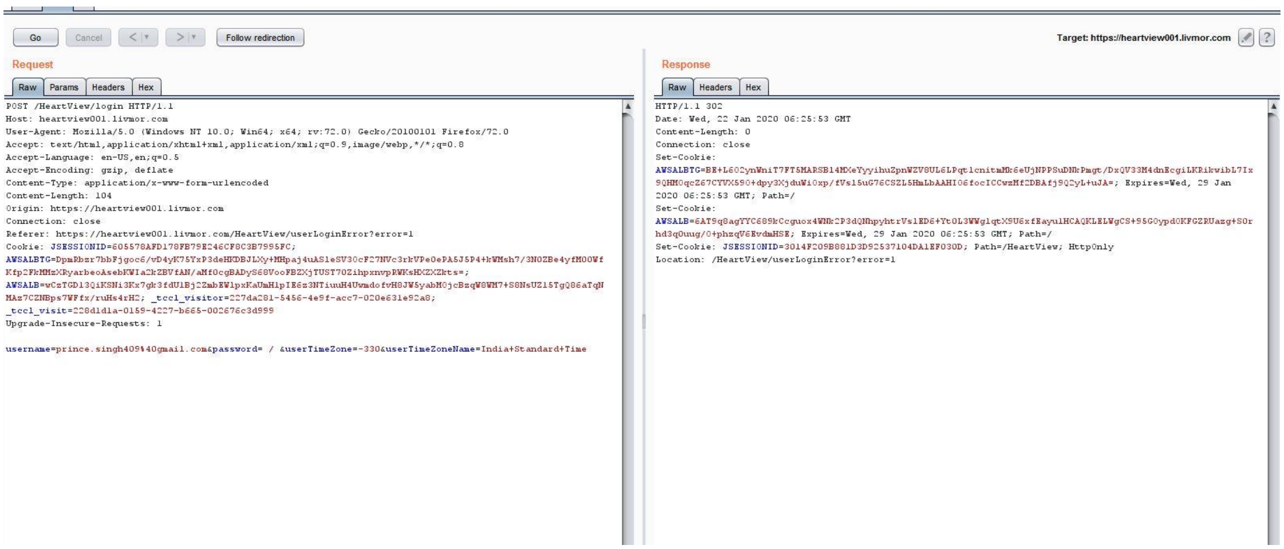
Password is tampered by adding a slash (patient's account)

Response in Browser



Invalid Username or Password. 3 attempt(s) before account locked.

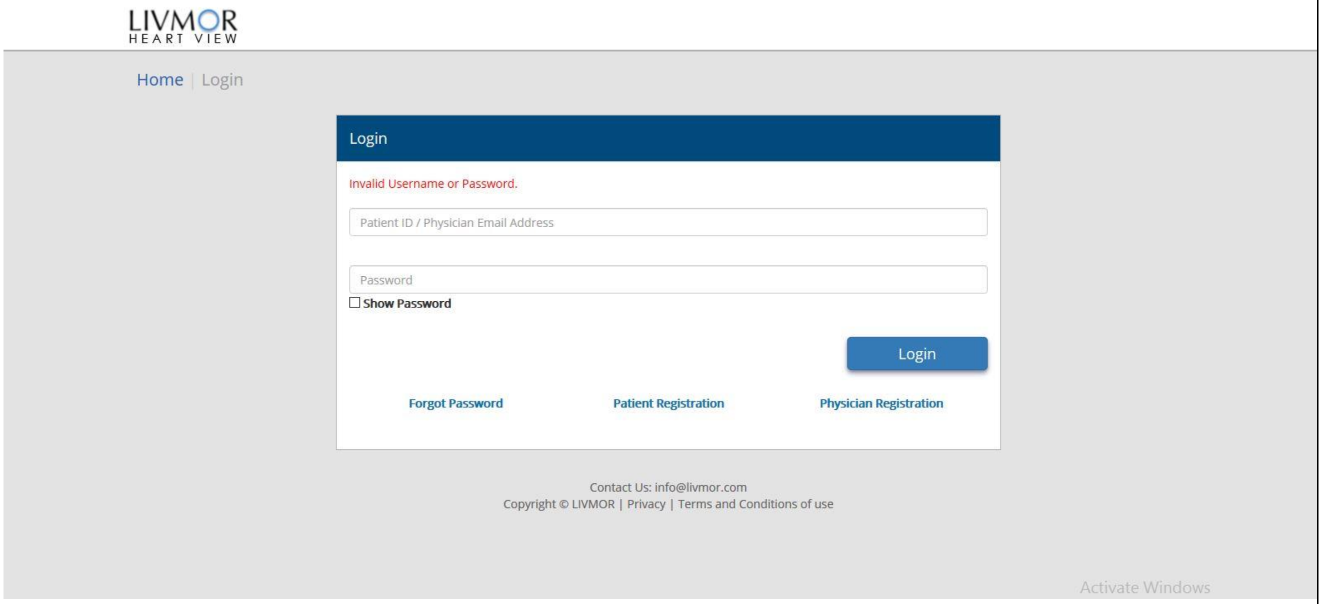
Error response received from the server indicating that the password has failed the pattern check



```
POST /HeartView/login HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Origin: https://heartview001.livmor.com
Connection: close
Referer: https://heartview001.livmor.com/HeartView/userLoginError?error=1
Cookie: JSESSIONID=605578AFD178FB79E246CF8C3B7995FC;
AWSALBTG=DpmRbzr7bbFjgoc6/vD4yK75YxP3deHKDBJLXy+MHpaj4uASleSV30cF27NVc3rkVPe0ePA5J5P4+kWMsh7/3N0ZBe4yfM00Wf
Kfp2FkMMzXRyarbeoAsebKWIa2kZBVfAN/aMf0cgBADyS68VooFBZXjTUST70ZihpxnvpRWKsHXZXZkts=;
AWSALB=wCzTGD13QiKSNi3Kx7gk3fdUlBj2ZmbEWlpxKaUmHlpIE6z3NTiuuH4UwmdofvH8JW5yabM0jcBzqW8WM7+S8NsUZ15TgQ86aTqN
MAz7CZNBps7WFfx/ruHs4rH2; _tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8;
_tccl_visit=228d1d1a-0159-4227-b665-002676c3d999
Upgrade-Insecure-Requests: 1

username=prince.singh409%40gmail.com&password= / &userTimeZone=-330&userTimeZoneName=India+Standard+Time
```

```
HTTP/1.1 302
Date: Wed, 22 Jan 2020 06:25:53 GMT
Content-Length: 0
Connection: close
Set-Cookie:
AWSALBTG=BE+L602ynWniT7FT5MARSB14MXeYyyihuZpnWZV8UL6LPqtlcnitmMk6eUjNPPSuDNkPmgt/DxQV33M4dnEcgiLKRikwibL7Ix
9QHM0qcZ67CYVX590+dpy3XjduWi0xp/fVsl5uG76CSZL5HmLbAAHI06focICCwzMf2DBAfj9Q2yL+uJA=; Expires=Wed, 29 Jan
2020 06:25:53 GMT; Path=/
Set-Cookie:
AWSALB=6AT9q8agYYC689kCcguox4WNk2P3dQNhpyhtrVslED6+Yt0L3WWglqtX9U6xfEayulHCAQKLELWgCS+95G0ypd0KFGZRUazg+S0r
hd3q0uug/0+phzqV6EvdmHSE; Expires=Wed, 29 Jan 2020 06:25:53 GMT; Path=/
Set-Cookie: JSESSIONID=3014F209B881D3D92537104DA1EF030D; Path=/HeartView; HttpOnly
Location: /HeartView/userLoginError?error=1
```

Password is tempered by adding a slash (physician's account)



Invalid Username or Password.

Contact Us: info@livmor.com
Copyright © LIVMOR | Privacy | Terms and Conditions of use

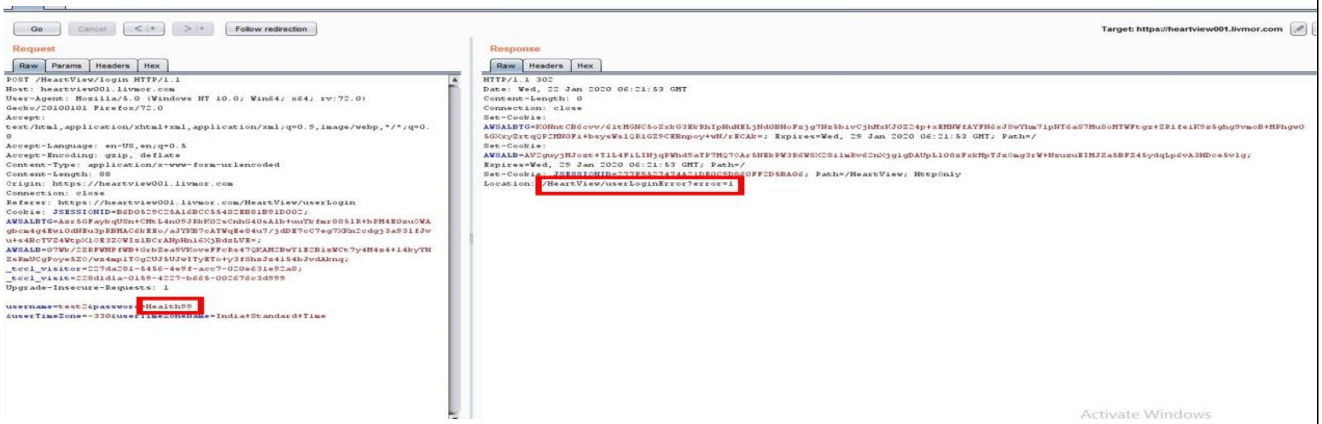
Error response received from the server indicating that the password has failed the pattern check

2.1.6 Server Side Password Complexity Check

Description: The password complexity check for the all user while registering/changing password is only performed at the browser side but not on the server side, by tampering the parameters through intercepting the request can bypass the complexity requirements and set any password of user’s own choice. User with penetration skills can bypass password complexity requirements.

Evidence

Request

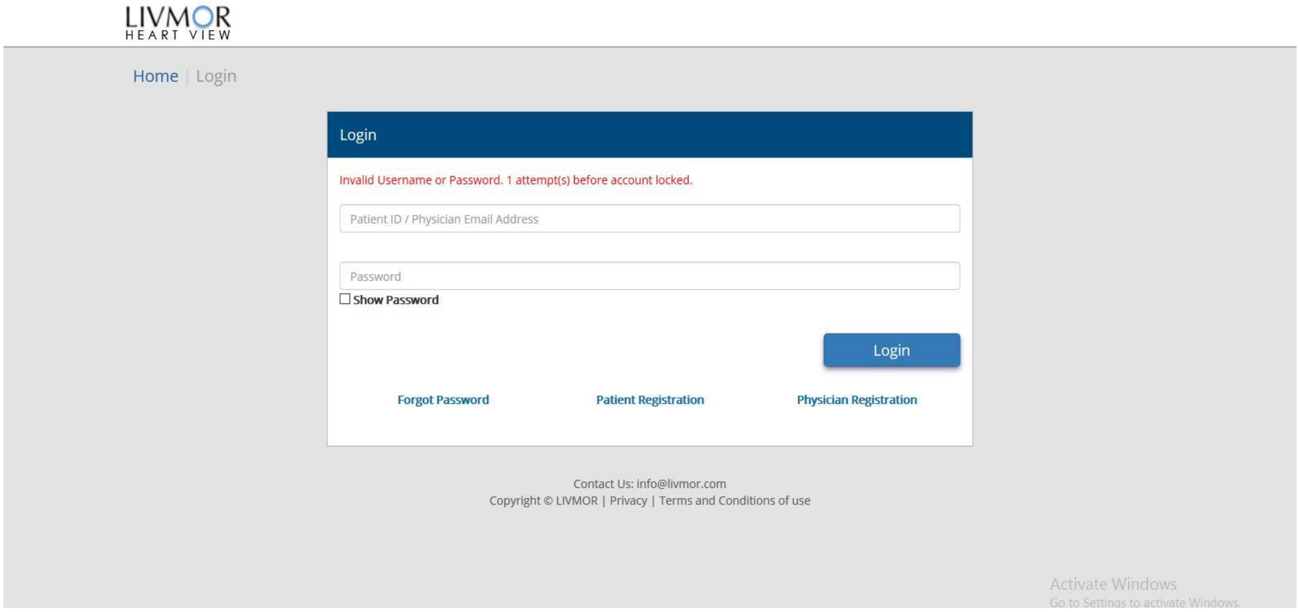


```
POST /HeartView/login HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Origin: https://heartview001.livmor.com
Connection: close
Referer: https://heartview001.livmor.com/HeartView/userLogin
Cookie: JSESSIONID=B6D0529C25A16BCC55402EB01B91D002;
AWSALBTG=Azr5GFaykqUSn+CMtL4n09JRkK02sCnhG40sA1b+uuYkfmr8851R+bPM4E0zu0WA
gbcm4g4Ewi0dNEu3pRBMAC6kEEo/aJYKB7cATWqEe84u7/jdDE7cC7eg7XKn2cdgj3a931fJv
u+s4BcTVZ4WtpX10E3Z0WIz1BCrANpHn16XjBdsLVE=;
AWSALB=07Wk/2ZRFWMPfWB+GrbZea9VKoveFFcRs47QKAM2BwY1E2B1zWCt7y4M4z4+14kyYH
ZsRmUCgPoye5Z0/wz4mp1T0g2UJ5UJwITyETo+y3fShzJz4154bJvdAknq;
_tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8;
_tccl_visit=228d1d1a-0159-4227-b665-002676e3d999
Upgrade-Insecure-Requests: 1

username=test2&password=Health99
&userTimeZone=-330&userTimeZoneName=India+Standard+Time
```

```
HTTP/1.1 302
Date: Wed, 22 Jan 2020 06:21:53 GMT
Content-Length: 0
Connection: close
Set-Cookie:
AWSALBTG=KONntCB6cvv/61tMGNC5oZxkG3EkRhIpHuHELjNd0BHoFzjg7Nz5bivCjhMxKJ0Z24p+xEMNWfAYFN6xJSwYhm71pNT6aS7MuSoMTWFtgz+ZRlfeiK9z5ghg9vmoB+MPhgw0
5GXxyZrtqQP2MN0Fi+bsysWs1QR1GZ9CEBnpoy+wN/rECAk=; Expires=Wed, 29 Jan 2020 06:21:53 GMT; Path=/
Set-Cookie:
AWSALB=AV2guyjMJozt+T1L4FiLINjqPWhd9aTP7MQ70ArSNEkPW3R6WSX20ilmRv62nXjglgDAUpL100zFxkMpTJz0mg3rW+NzuzuEIMJZa6BFZ45ydqLp6vA3HDce5v1g;
Expires=Wed, 29 Jan 2020 06:21:53 GMT; Path=/
Set-Cookie: JSESSIONID=277F8527474A21DE0C5D860FF2D5BA06; Path=/HeartView; HttpOnly
Location: /HeartView/userLoginError?error=1
```

Providing changed & expected password by application. (Patient’s account)

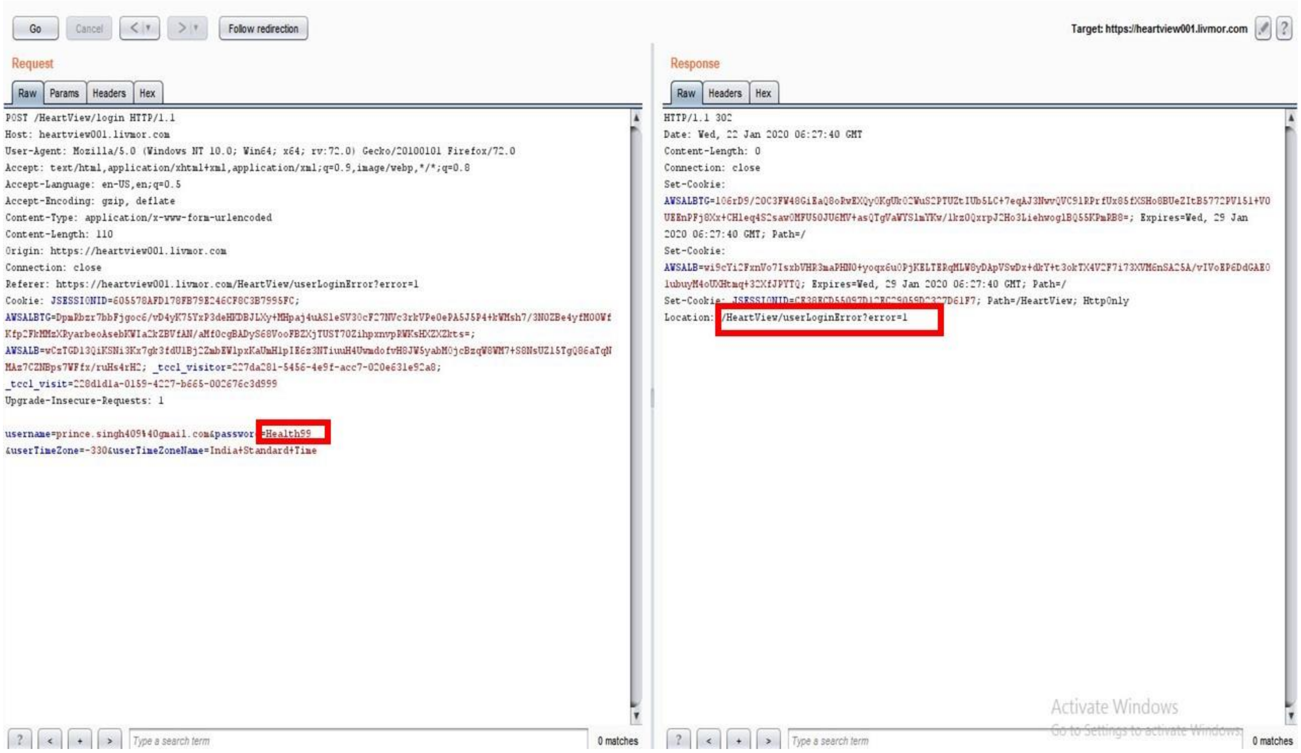
Response In Browser



Invalid Username or Password. 1 attempt(s) before account locked.

Contact Us: info@livmor.com
Copyright © LIVMOR | Privacy | Terms and Conditions of use

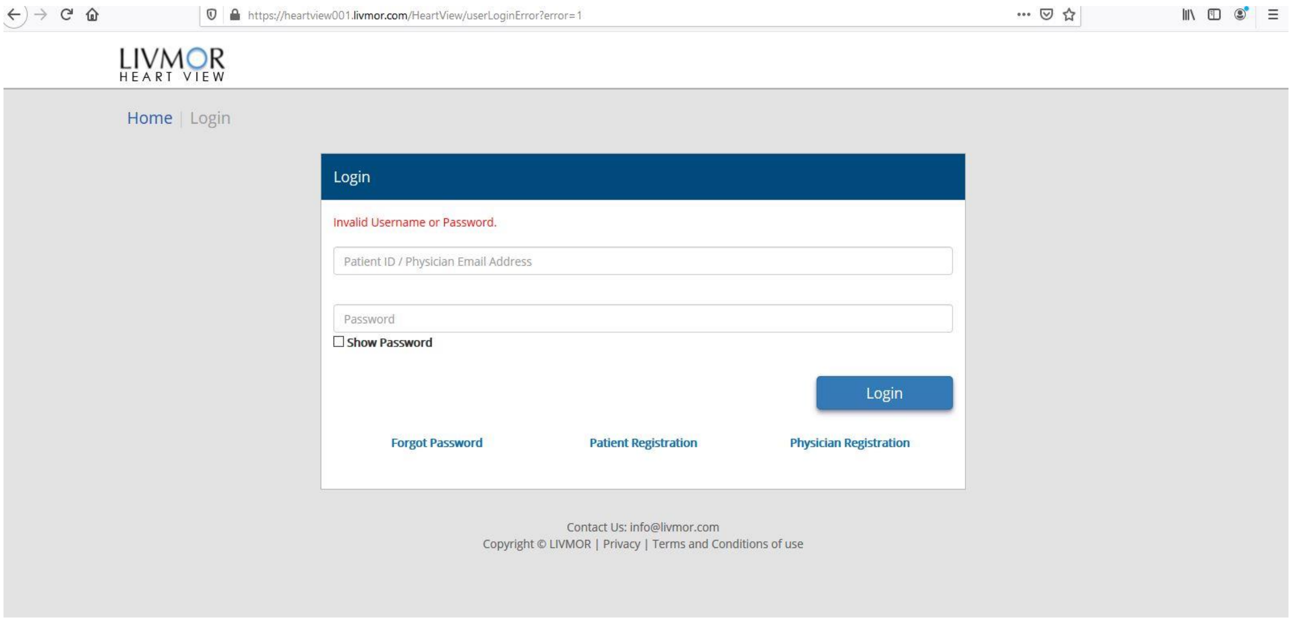
After rendering, it again redirects to the login page.



```
POST /HeartView/login HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 110
Origin: https://heartview001.livmor.com
Connection: close
Referer: https://heartview001.livmor.com/HeartView/userLoginError?error=1
Cookie: JSESSIONID=605578AFD178FB79E246CF8C3B7995FC;
AWSALBTG=DpmRbzr7bbFjgoc6/vD4yK75YxP3deHKDBJLXy+MHpaj4uAS1eSV30cF27NVc3rkVPeOePA5J5P4+kWMsh7/3N0ZBe4yfM00Wf
Kfp2FkMMzXRyarbeoAsebKWIa2kZBVfAN/aMf0cgBADyS68VooFBZXjTUST70ZihpxnvpRWKsHXZXZkts=;
AWSALB=wCzTGD13QiKSNi3Kx7gk3fdU1Bj2ZmbEW1pxKaUmHlpIE6z3NTiuuH4UwmdofvH8JW5yabM0jcBzqW8WM7+S8NsUZ15TgQ86aTqN
MAz7CZNBps7WFfx/ruHs4rH2; _tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8;
_tccl_visit=228d1d1a-0159-4227-b665-002676c3d999
Upgrade-Insecure-Requests: 1

username=prince.singh409%40gmail.com&password=Health99
&userTimeZone=-330&userTimeZoneName=India+Standard+Time
```

```
HTTP/1.1 302
Date: Wed, 22 Jan 2020 06:27:40 GMT
Content-Length: 0
Connection: close
Set-Cookie:
AWSALBTG=106rD9/20C3FW48GiEaQ8oRwEXQy0KgUk02WuS2PTUZtIUb5LC+7eqAJ3NwvQVC91RPrfUx85fXSHo8BUeZItB5772PV151+V0
UEEnPFj8Xx+CHleq4S2saw0MFU50JU6MV+asQTgVaWYS1mYKw/1kz0QxrpJ2Ho3LiehwoglBQ55KPmRB8=; Expires=Wed, 29 Jan
2020 06:27:40 GMT; Path=/
Set-Cookie:
AWSALB=wi9cYi2FxnVo7IsxbVHR3maPHN0+yoqx6u0PjKELTERqMLW8yDApVSwDx+dkY+t3okTX4V2F7i73XVM6nSA25A/vIVoEP6DdGAE0
1ubuyM4oUXHtmq+32XfJPYTQ; Expires=Wed, 29 Jan 2020 06:27:40 GMT; Path=/
Set-Cookie: JSESSIONID=CE38ECD55097D12EC29059D2327D61F7; Path=/HeartView; HttpOnly
Location: /HeartView/userLoginError?error=1
```

Providing changed & expected password by application. (Physician's account)



Invalid Username or Password.

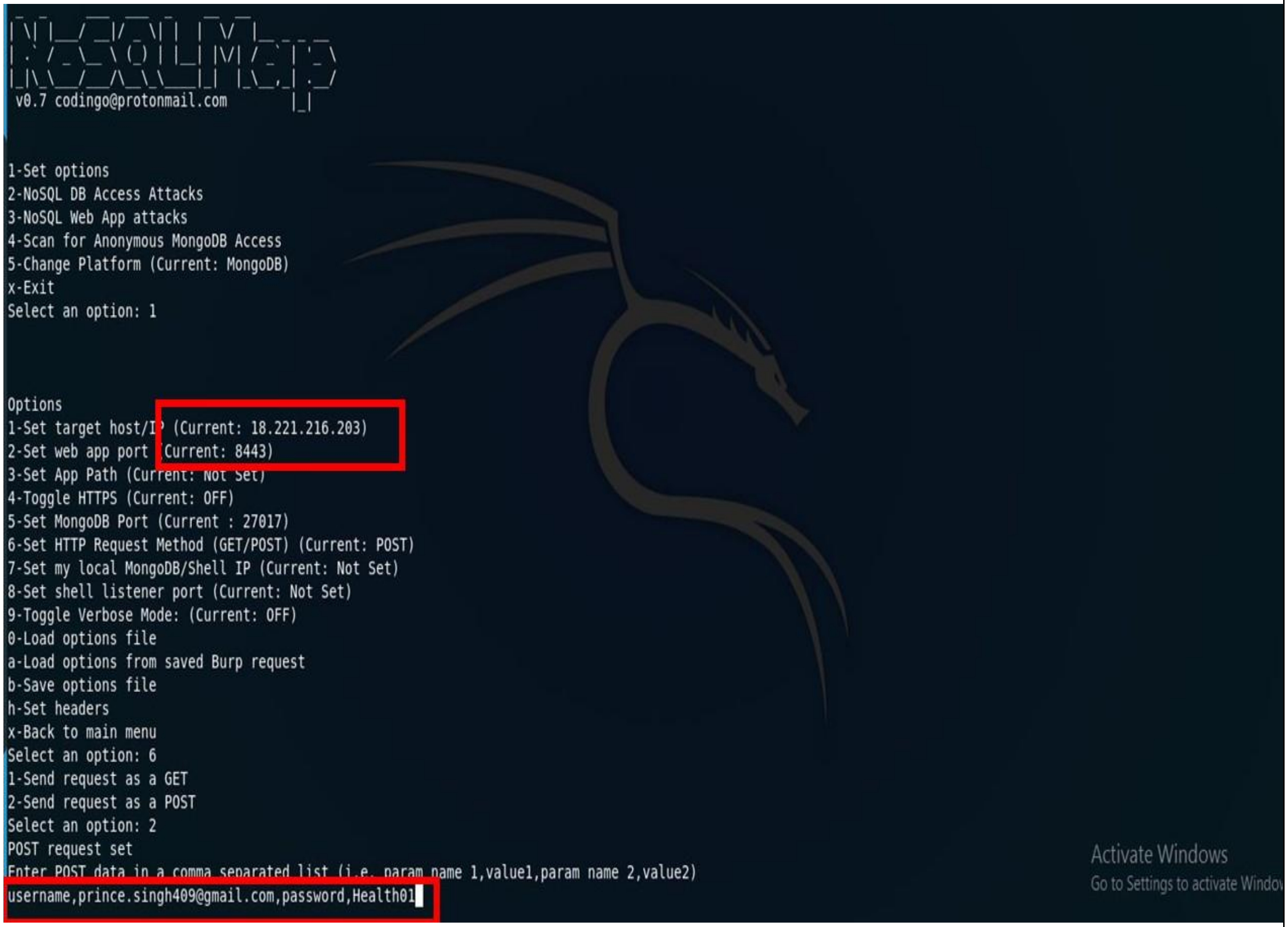
Contact Us: info@livmor.com
Copyright © LIVMOR | Privacy | Terms and Conditions of use

After rendering, it again redirects to the login page.

2.1.7 NoSQL Injection

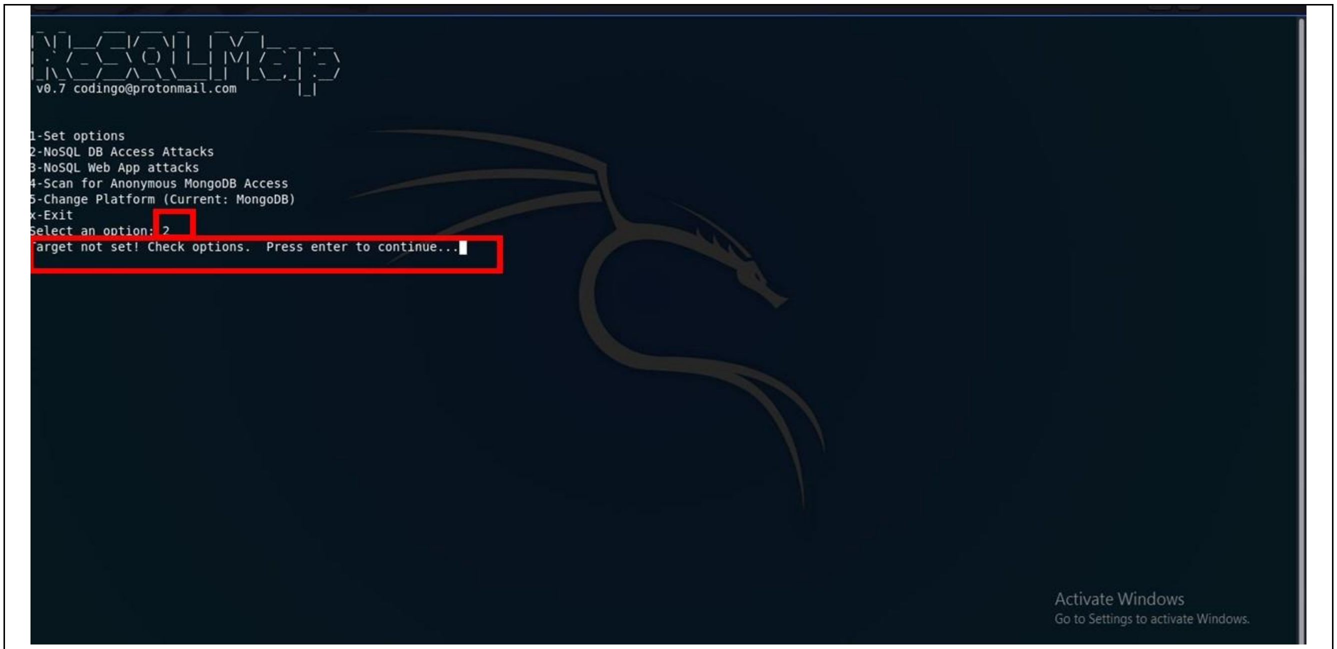
Description: NoSQL Injection is security vulnerability that lets attackers take control of database queries through the unsafe use of user input. It can be used by an attacker to: Expose unauthorized information. Modify data.

Evidence



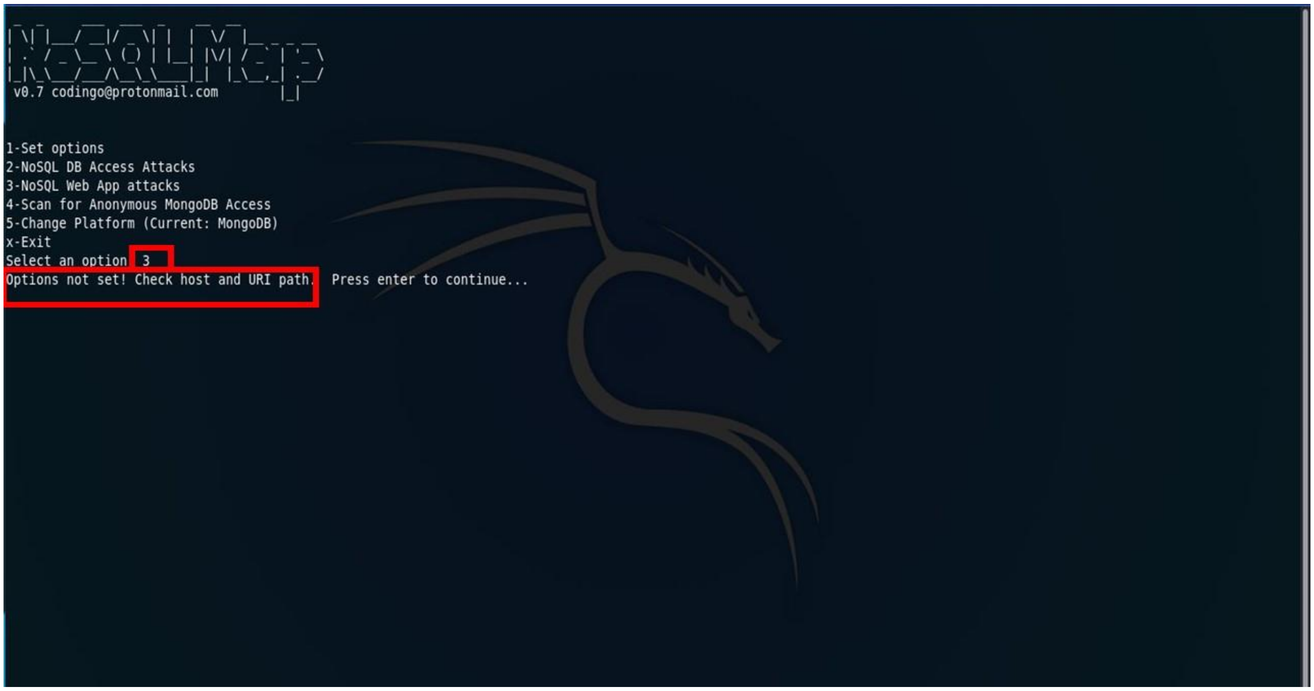
```
 _   _       ____   ___  _     __  __
| \ | | ___/ ___| / _ \| |   |  \/  | __ _ _ __
|  \| |/ _ \___ \| | | | |   | |\/| |/ _` | '_ \
| |\  | (_) |__) | |_| | |___| |  | | (_| | |_) |
|_| \_|\___/____/ \__\_\_____|_|  |_|\__,_| .__/
 v0.7 codingo@protonmail.com               |_|


1-Set options
2-NoSQL DB Access Attacks
3-NoSQL Web App attacks
4-Scan for Anonymous MongoDB Access
5-Change Platform (Current: MongoDB)
x-Exit
Select an option: 1


Options
1-Set target host/IP (Current: 18.221.216.203)
2-Set web app port (Current: 8443)
3-Set App Path (Current: Not Set)
4-Toggle HTTPS (Current: OFF)
5-Set MongoDB Port (Current : 27017)
6-Set HTTP Request Method (GET/POST) (Current: POST)
7-Set my local MongoDB/Shell IP (Current: Not Set)
8-Set shell listener port (Current: Not Set)
9-Toggle Verbose Mode: (Current: OFF)
0-Load options file
a-Load options from saved Burp request
b-Save options file
h-Set headers
x-Back to main menu
Select an option: 6
1-Send request as a GET
2-Send request as a POST
Select an option: 2
POST request set
Enter POST data in a comma separated list (i.e. param name 1,value1,param name 2,value2)
username,prince.singh409@gmail.com,password,Health01
```

Set the IP address, port and data.



```
 v0.7 codingo@protonmail.com


1-Set options
2-NoSQL DB Access Attacks
3-NoSQL Web App attacks
4-Scan for Anonymous MongoDB Access
5-Change Platform (Current: MongoDB)
x-Exit
Select an option: 2
Target not set! Check options.  Press enter to continue...
```

Try with DB Access Attacks by providing option 2. Getting Target Not set.



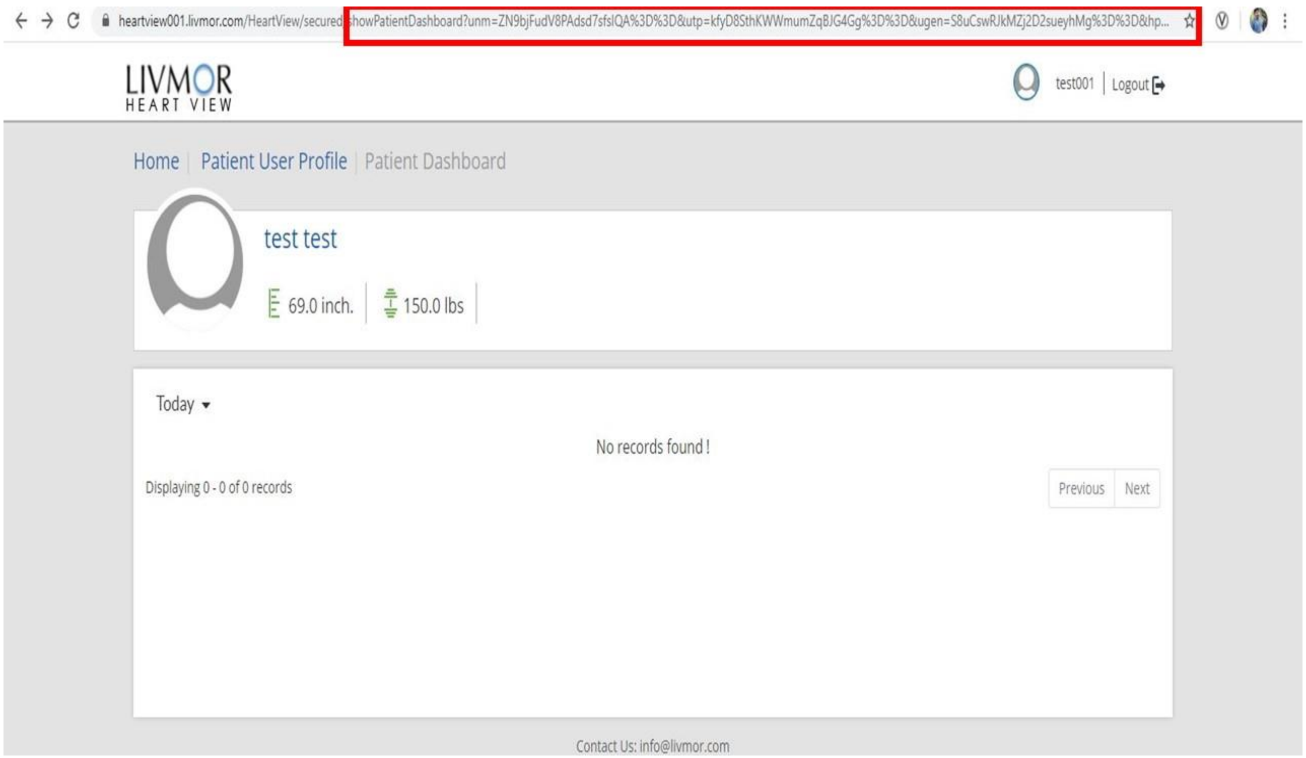
```
 v0.7 codingo@protonmail.com


1-Set options
2-NoSQL DB Access Attacks
3-NoSQL Web App attacks
4-Scan for Anonymous MongoDB Access
5-Change Platform (Current: MongoDB)
x-Exit
Select an option: 3
Options not set! Check host and URI path.  Press enter to continue...
```

Not able to connect to the target. Exploit cannot be performed.

2.1.8 Insecure Direct Object Reference

Description: Insecure Direct Object References occur when an application provides direct access to objects based on user-supplied input. Because of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files. Insecure Direct Object References allow attackers to bypass authorization and access resources directly by modifying the value of a parameter used to directly point to an object. Such resources can be database entries belonging to other users, files in the system, and more. This is caused by the fact that the application takes user supplied input and uses it to retrieve an object without performing sufficient authorization checks.

Evidence



heartview001.livmor.com/HeartView/secured/showPatientDashboard?unm=ZN9bjFudV8PAdsd7sfsIQA%3D%3D&utp=kfyD8SthKWWmumZqBJG4Gg%3D%3D&ugen=S8uCswRJkMZj2D2sueyhMg%3D%3D&hp...

test test

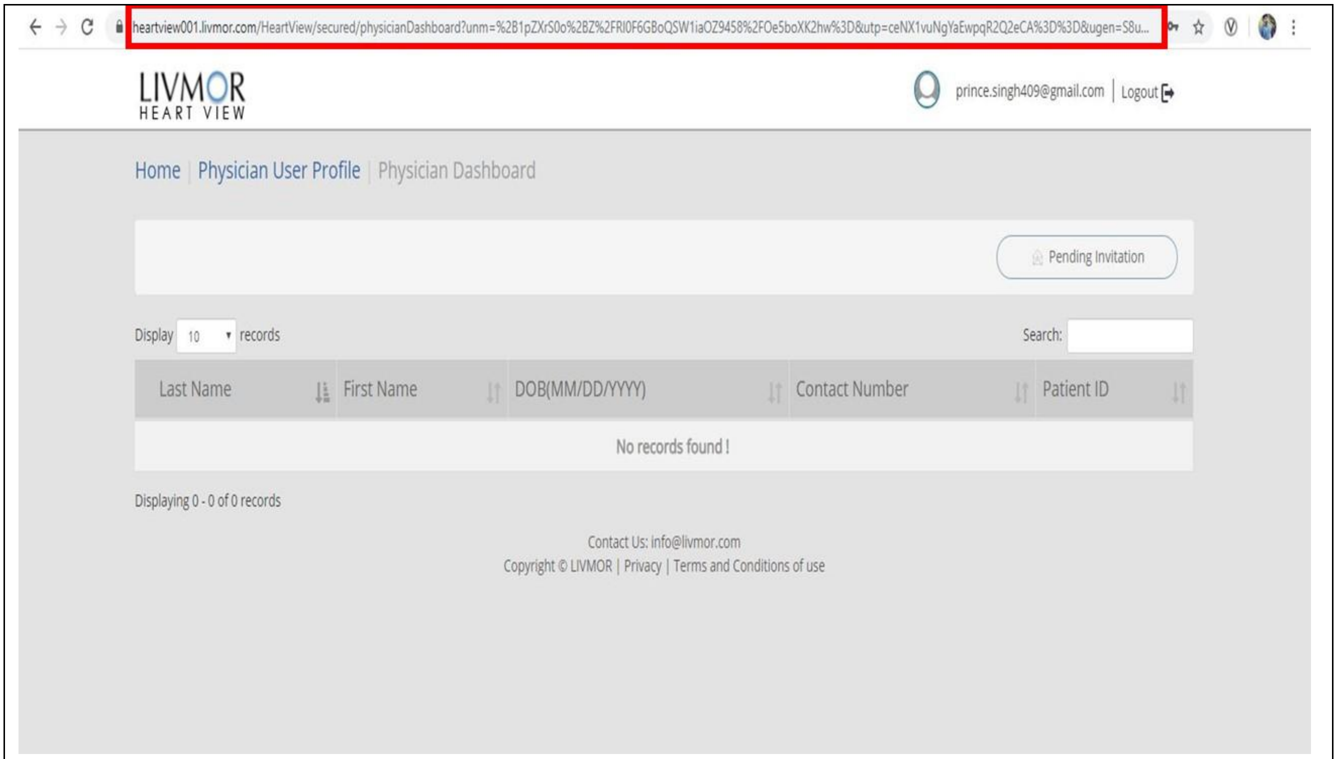
69.0 inch. | 150.0 lbs

No records found !

Displaying 0 - 0 of 0 records

Contact Us: info@livmor.com

Encrypted URL prevents from tampering the data fields (Patient's account)



heartview001.livmor.com/HeartView/secured/physicianDashboard?unm=%2B1pZXrS0o%2BZ%2FRI0F6GBoQSW1iaOZ9458%2FOe5boXK2hw%3D&utp=ceNX1vuNgYaEwpqR2Q2eCA%3D%3D&ugen=S8u...

Last Name	First Name	DOB(MM/DD/YYYY)	Contact Number	Patient ID
No records found !				

Displaying 0 - 0 of 0 records

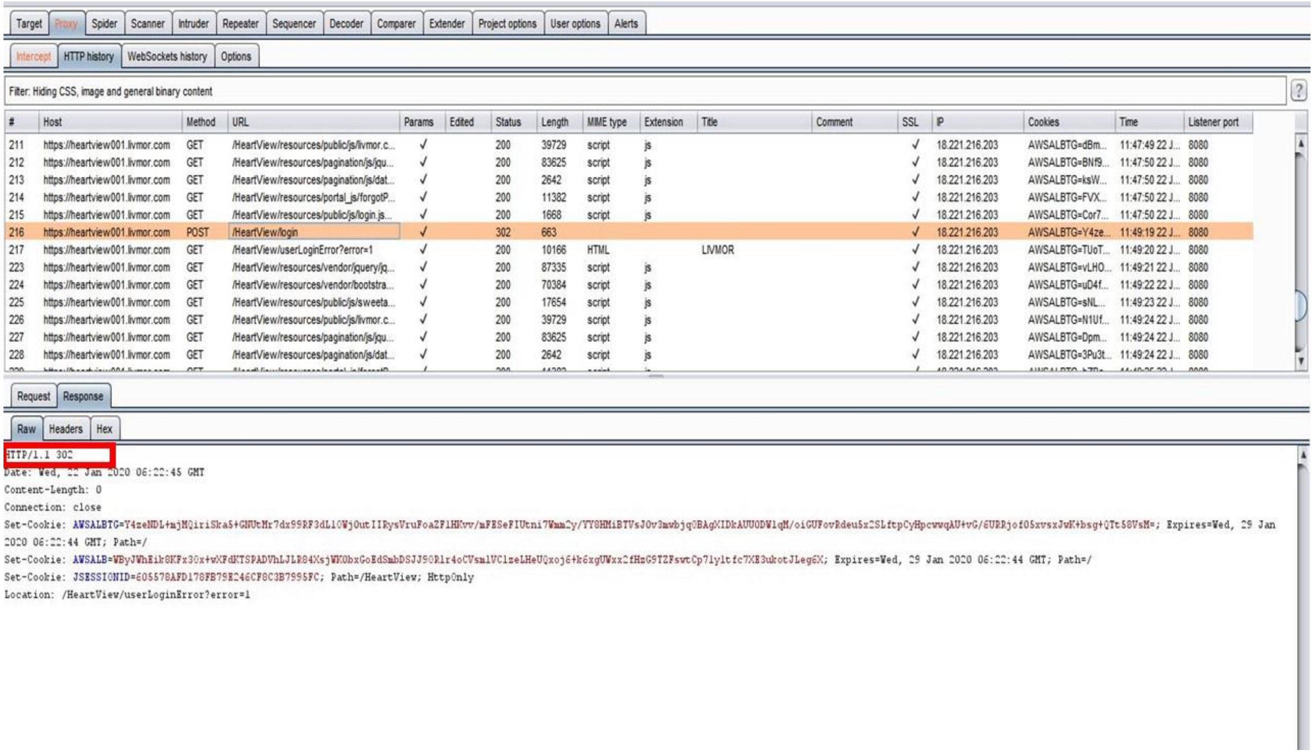
Contact Us: info@livmor.com
Copyright © LIVMOR | Privacy | Terms and Conditions of use

Encrypted URL prevents from tampering the data fields (Physician's account)

2.1.9 Server Banner Disclosure

Description: The HTTP responses returned by this web application include a header named Server. The value of this header includes the version of Apache server.

Evidence



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
211	https://heartview001.livmor.com	GET	/HeartView/resources/public/js/livmor.c...	✓		200	39729	script	js			✓	18.221.216.203	AWSALBTG=dBm...	11:47:49 22 J...	8080
212	https://heartview001.livmor.com	GET	/HeartView/resources/pagination/js/jqu...	✓		200	83625	script	js			✓	18.221.216.203	AWSALBTG=BNf9...	11:47:50 22 J...	8080
213	https://heartview001.livmor.com	GET	/HeartView/resources/pagination/js/dat...	✓		200	2642	script	js			✓	18.221.216.203	AWSALBTG=ksW...	11:47:50 22 J...	8080
214	https://heartview001.livmor.com	GET	/HeartView/resources/portal_js/forgotP...	✓		200	11382	script	js			✓	18.221.216.203	AWSALBTG=FVX...	11:47:50 22 J...	8080
215	https://heartview001.livmor.com	GET	/HeartView/resources/public/js/login.js...	✓		200	1668	script	js			✓	18.221.216.203	AWSALBTG=Cor7...	11:47:50 22 J...	8080
216	https://heartview001.livmor.com	POST	/HeartView/login	✓		302	663					✓	18.221.216.203	AWSALBTG=Y4ze...	11:49:19 22 J...	8080
217	https://heartview001.livmor.com	GET	/HeartView/userLoginError?error=1	✓		200	10166	HTML		LIVMOR		✓	18.221.216.203	AWSALBTG=TUoT...	11:49:20 22 J...	8080
223	https://heartview001.livmor.com	GET	/HeartView/resources/vendor/jquery/jq...	✓		200	87335	script	js			✓	18.221.216.203	AWSALBTG=vLHO...	11:49:21 22 J...	8080
224	https://heartview001.livmor.com	GET	/HeartView/resources/vendor/bootstra...	✓		200	70384	script	js			✓	18.221.216.203	AWSALBTG=uD4f...	11:49:22 22 J...	8080
225	https://heartview001.livmor.com	GET	/HeartView/resources/public/js/sweeta...	✓		200	17654	script	js			✓	18.221.216.203	AWSALBTG=sNL...	11:49:23 22 J...	8080
226	https://heartview001.livmor.com	GET	/HeartView/resources/public/js/livmor.c...	✓		200	39729	script	js			✓	18.221.216.203	AWSALBTG=N1Uf...	11:49:24 22 J...	8080
227	https://heartview001.livmor.com	GET	/HeartView/resources/pagination/js/jqu...	✓		200	83625	script	js			✓	18.221.216.203	AWSALBTG=Dpm...	11:49:24 22 J...	8080
228	https://heartview001.livmor.com	GET	/HeartView/resources/pagination/js/dat...	✓		200	2642	script	js			✓	18.221.216.203	AWSALBTG=3Pu3t...	11:49:24 22 J...	8080

```
HTTP/1.1 302
Date: Wed, 22 Jan 2020 06:22:45 GMT
Content-Length: 0
Connection: close
Set-Cookie: AWSALBTG=Y4zeNDL+mjMQiriSka5+GNUtMr7dx99RF3dL10Wj0utIIRysVruFoaZF1HKvv/mFESeFIUtni7Wmm2y/YY8HMiBTVsJOv3mwbjq0BAgXIDkAUU0DW1qM/oiGUFovRdeu5x2SLftpCyHpcwwqAU+vG/6URRjof05xvsxJwK+bsg+QTt58VsM=; Expires=Wed, 29 Jan
2020 06:22:44 GMT; Path=/
Set-Cookie: AWSALB=WByJWhEik8KFx30x+wXFdKTSPADVhLJLR84XsjWK0bxGoEdSmbDSJJ90Rlr4oCVsmlVClzeLHeUQxoj6+k6xgUWxx2fHzG9TZFswtCp7lyltfc7XE3ukotJLeg6X; Expires=Wed, 29 Jan 2020 06:22:44 GMT; Path=/
Set-Cookie: JSESSIONID=605578AFD178FB79E246CF8C3B7995FC; Path=/HeartView; HttpOnly
Location: /HeartView/userLoginError?error=1
```

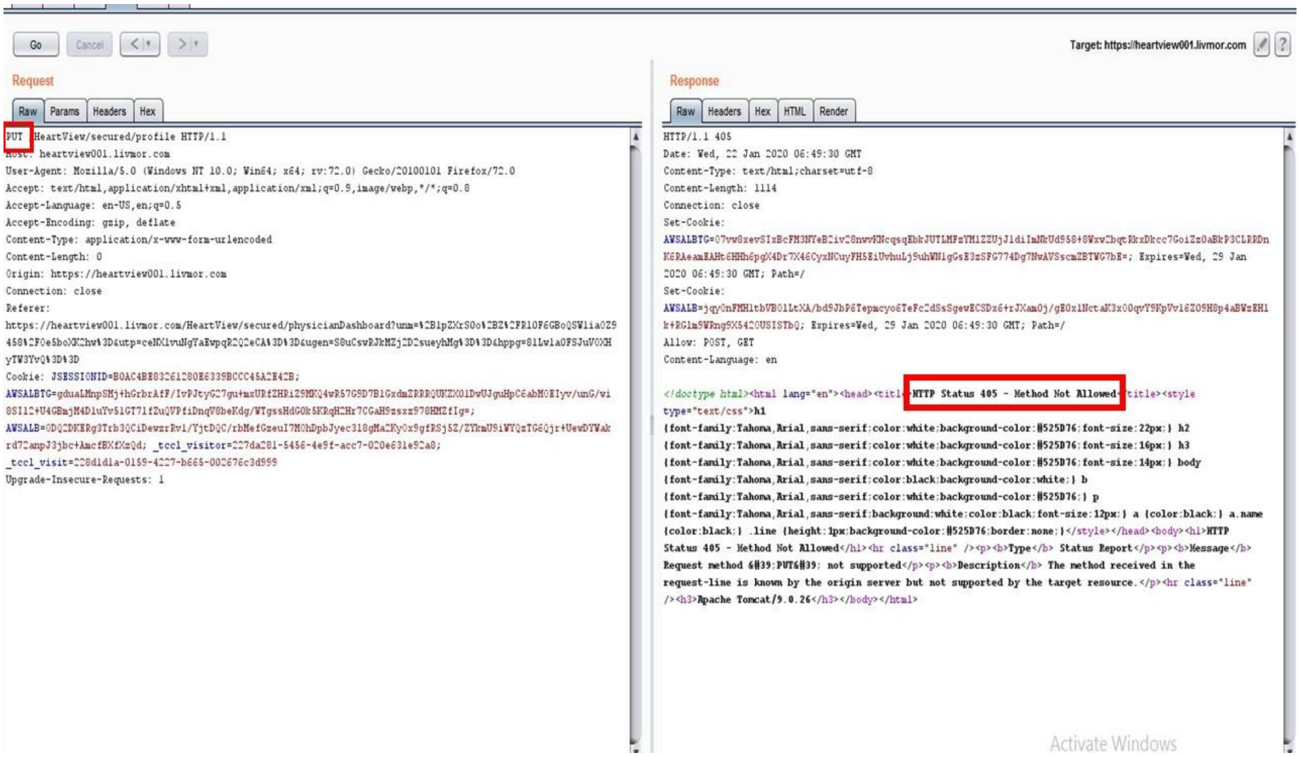
No information about the server is found in the response

2.1.10 Insecure HTTP Methods Enabled

Description: HTTP offers many methods that can be used to perform actions on the web server. Many of these methods are designed to aid developers in deploying and testing HTTP applications. These HTTP methods can be used for nefarious purposes if the web server is misconfigured. Some of these methods can potentially pose a security risk for a web application, as they allow an attacker to modify the files stored on the web server.

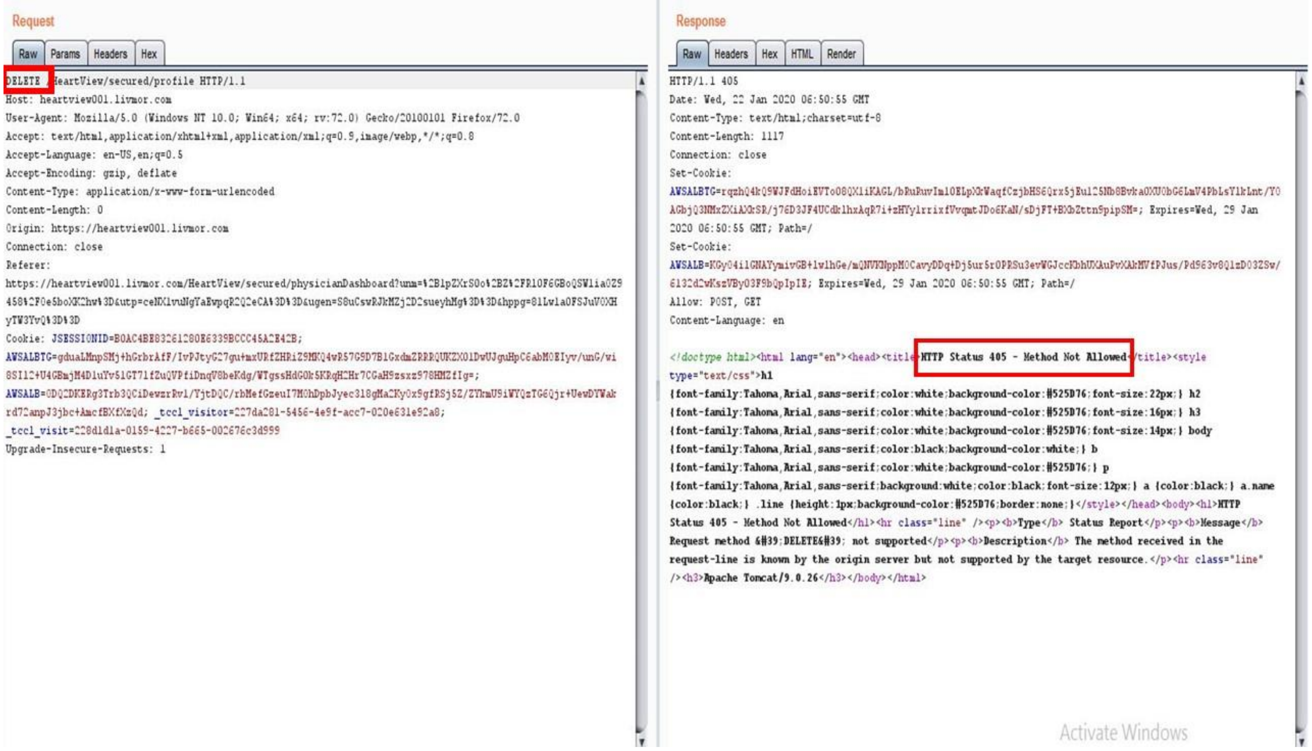
- PUT: This method allows a client to upload new files on the web server. An attacker can exploit it by uploading malicious files (e.g.: an asp file that executes commands by invoking cmd.exe), or by simply using the victim's server as a file repository.
- DELETE: This method allows a client to delete a file on the web server. An attacker can exploit it as a very simple and direct way to deface a web site or to mount a Denial-of-Service attack.
- Head, trace, options, patch are also allowed in this instance. These methods if not needed by the application then it must be disabled either through the application or at the server level.

Evidence



```
PUT HeartView/secured/profile HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: https://heartview001.livmor.com
Connection: close
Referer:
https://heartview001.livmor.com/HeartView/secured/physicianDashboard?unm=%2BlpZXrS0o%2BZ%2FR10F6GBoQSWlia0Z9
458%2F0e5boXK2hw%3D&utp=ceNXlvuNgYaEwpqR2Q2eCA%3D%3D&ugen=S8uCswRJkMZj2D2sueyhMg%3D%3D&hppg=81Lwla0FSJuV0XH
yTW3YvQ%3D%3D
Cookie: JSESSIONID=B0AC4BE83261280E6339BCCC45A2E42B;
AWSALBTG=gduaLMnpSMj+hGrbrAfF/IvPJtyG27gu+mxURfZHRiZ9MKQ4wR57G9D7B1GxdmZRRRQUKZX01DwUJguHpC6abM0EIyv/unG/wi
8SI12+U4GBmjM4DluYv51GT71fZuQVPfiDnqV8beKdg/WTgssHdG0k5KRqH2Hr7CGaH9zsxz978HMZfIg=;
AWSALB=0DQ2DKERg3Trb3QCiDewzrRv1/YjtDQC/rbMefGzeuI7M0hDpbJyec318gMa2Ky0x9gfRSj5Z/ZYkmU9iWYQzTG6Qjr+UewDYWak
rd72anpJ3jbc+AmcfBXfXzQd; _tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8;
_tccl_visit=228d1d1a-0159-4227-b665-002676c3d999
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 405
Date: Wed, 22 Jan 2020 06:49:30 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 1114
Connection: close
Set-Cookie:
AWSALBTG=07vw8xevSIxBcFM3NYeB2iv28nwvKNcqsqEbkJUTLMFzYM1ZZUjJ1diImNkUd958+8Wxw2bqtRkxDkcc7GoiZz0aBkP3CLRRDn
K6RAeamEAHt6HHh6pgX4Dr7X46CyxNCuyFH5EiUvhuLj9uhWNlgGsE3zSFG774Dg7NwAVSscmZBTWG7bE=; Expires=Wed, 29 Jan
2020 06:49:30 GMT; Path=/
Set-Cookie:
AWSALB=jqy0nFMHltbVB01LtXA/bd9JbP6Tepmcyo6TeFc2dSsSgewECSDx6+rJXam0j/gE0xlNctaK3x00qvY9KpVvl6Z09H8p4aBWzEHl
k+RGlm9WRng9X5420USISTbQ; Expires=Wed, 29 Jan 2020 06:49:30 GMT; Path=/
Allow: POST, GET
Content-Language: en

<!doctype html><html lang="en"><head><title>HTTP Status 405 - Method Not Allowed</title><style
type="text/css">h1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} h2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} h3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} body
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} b
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;} a {color:black;} a.name
{color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP
Status 405 - Method Not Allowed</h1><hr class="line" /><p><b>Type</b> Status Report</p><p><b>Message</b>
Request method &#39;PUT&#39; not supported</p><p><b>Description</b> The method received in the
request-line is known by the origin server but not supported by the target resource.</p><hr class="line"
/><h3>Apache Tomcat/9.0.26</h3></body></html>
```



```
DELETE /HeartView/secured/profile HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: https://heartview001.livmor.com
Connection: close
Referer:
https://heartview001.livmor.com/HeartView/secured/physicianDashboard?unm=%2BlpZXrS0o%2BZ%2FRl0F6GBoQSWlia0Z9
458%2F0e5boXK2hw%3D&utp=ceNX1vuNgYaEwpqR2Q2eCA%3D%3D&ugen=S8uCswRJkMZj2D2sueyhMg%3D%3D&hppg=81Lwla0FSJuV0XH
yTW3YvQ%3D%3D
Cookie: JSESSIONID=B0AC4BE83261280E6339BCCC45A2E42B;
AWSALBTG=gduaLMnpSMj+hGrbrAfF/IvPJtyG27gu+mxURfZHRiZ9MKQ4wR57G9D7B1GxdmZRRRQUKZX01DwUJguHpC6abM0EIyv/unG/wi
8SI12+U4GBmjM4DluYv51GT71fZuQVPfiDnqV8beKdg/WTgssHdG0k5KRqH2Hr7CGaH9zsxz978HMZfIg=;
AWSALB=0DQ2DKERg3Trb3QCiDewzrRvl/YjtDQC/rbMefGzeuI7M0hDpbJyec318gMa2Ky0x9gfRSj5Z/ZYkmU9iWYQzTG6Qjr+UewDYWak
rd72anpJ3jbc+AmcfBXfXzQd; _tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8;
_tccl_visit=228d1d1a-0159-4227-b665-002676c3d999
Upgrade-Insecure-Requests: 1
```

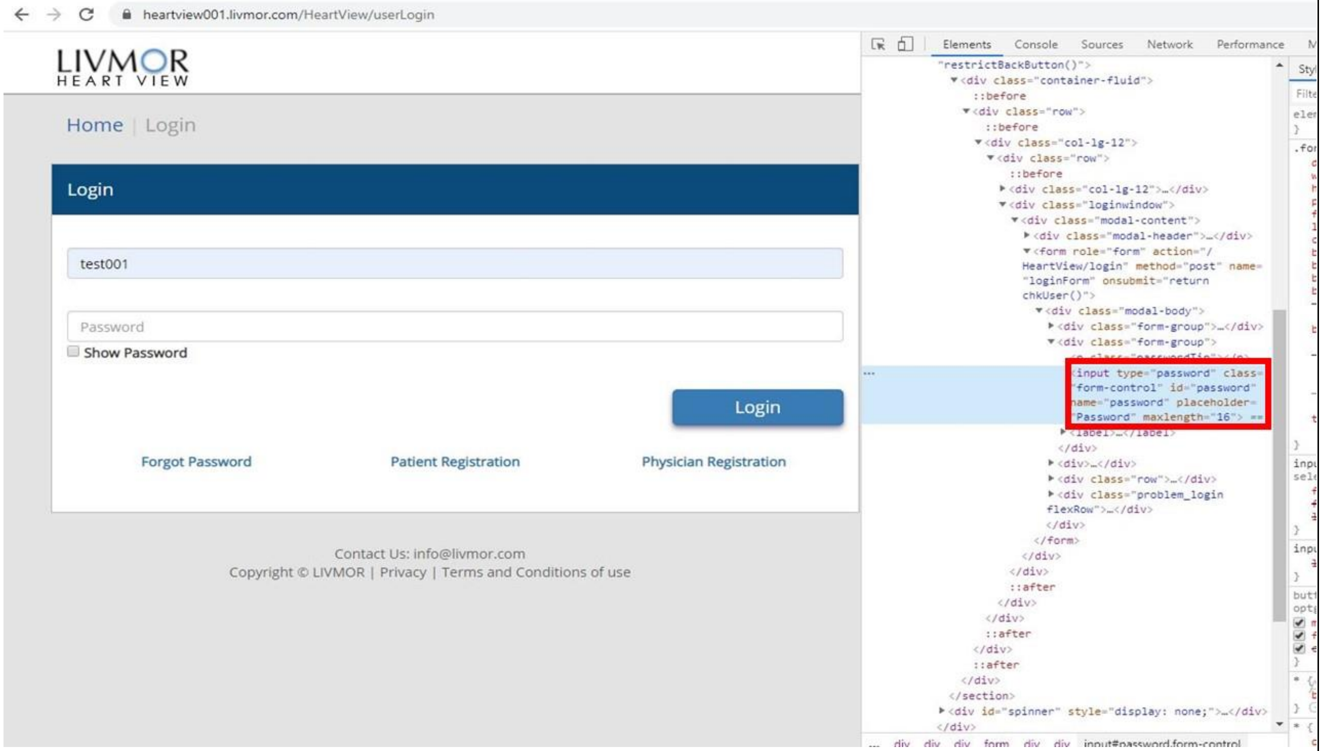
```
HTTP/1.1 405
Date: Wed, 22 Jan 2020 06:50:55 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 1117
Connection: close
Set-Cookie:
AWSALBTG=rqzhQ4kQ9WJFdHoiEVTo08QX1iKAGL/bRuRuvIm10ELpXkWaqfCzjbHS6Qrx5jEul25Nb8Bvka0XU0bG6LmV4PbLsY1kLnt/Y0
AGbjQ3NMxZXiAXkSR/j76D3JF4UCdklhxAqR7i+zHYylrrixfVvqmtJDo6KaN/sDjFT+BXbZttn9pipSM=; Expires=Wed, 29 Jan
2020 06:50:55 GMT; Path=/
Set-Cookie:
AWSALB=KGy04ilGNAYymivGB+lwlhGe/mQNVKNppM0CavyDDq+Dj5ur5r0PRSu3evWGJccKbhUXAuPvXAkMVfPJus/Pd963v8QlzD03ZSw/
6132d2wKszVBy03F9bQpIpIE; Expires=Wed, 29 Jan 2020 06:50:55 GMT; Path=/
Allow: POST, GET
Content-Language: en

<!doctype html><html lang="en"><head><title>HTTP Status 405 - Method Not Allowed</title><style
type="text/css">h1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} h2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} h3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} body
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} b
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;} a {color:black;} a.name
{color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP
Status 405 - Method Not Allowed</h1><hr class="line" /><p><b>Type</b> Status Report</p><p><b>Message</b>
Request method &#39;DELETE&#39; not supported</p><p><b>Description</b> The method received in the
request-line is known by the origin server but not supported by the target resource.</p><hr class="line"
/><h3>Apache Tomcat/9.0.26</h3></body></html>
```

The HTTP Methods are not allowed.

2.1.11 Password Autocomplete in Browser

Description: Browsers asking the user to remember the password that they have. The browser will then store the password, and automatically enter it whenever the same authentication form is visited. This is a convenience for the user. Additionally, custom "remember me" functionality allow users to persist log ins on a specific client system. Having the browser store passwords is not only a convenience for end-users, but also for an attacker. If an attacker can gain access to the victim's browser (e.g. through a Cross Site Scripting attack, or through a shared computer), then they can retrieve the stored passwords.

Evidence



Username: test001

```
"restrictBackButton()">
  ▼<div class="container-fluid">
     ::before
   ▼<div class="row">
       ::before
     ▼<div class="col-lg-12">
       ▼<div class="row">
           ::before
         ▶<div class="col-lg-12">…</div>
         ▼<div class="loginwindow">
           ▼<div class="modal-content">
             ▶<div class="modal-header">…</div>
             ▼<form role="form" action="/
             HeartView/login" method="post" name=
             "loginForm" onsubmit="return
             chkUser()">
               ▼<div class="modal-body">
                 ▶<div class="form-group">…</div>
                 ▼<div class="form-group">
                     <input type="password" class=
                     "form-control" id="password"
                     name="password" placeholder=
                     "Password" maxlength="16"> ==
                   ▶<label>…</label>
                   </div>
                 ▶<div>…</div>
                 ▶<div class="row">…</div>
                 ▶<div class="problem_login
                 flexRow">…</div>
                 </div>
               </form>
             </div>
           </div>
           ::after
         </div>
       </div>
       ::after
     </div>
     ::after
   </div>
  </section>
 ▶<div id="spinner" style="display: none;">…</div>
 </div>
... div div div form div div input#password.form-control
```

No Alert Message for Password Autocomplete in Browser

3. Vulnerabilities explained in detail

3.1 Concurrent Session Remain Active

Name	Concurrent session remains active after password change	**Impact**	Medium	**Risk Rating**	Medium
Ease of Exploit	Easy	**Likelihood**	Medium		
Category	Session Management				
URL / Impacted System	All Users				

Description

Concurrent session control amounts to controlling the number of sessions a user can have at the same time. Normally, each user has his own account, so it's logical that a user can be logged in only once at a time. Since users might use different devices you might want to allow more than one session, but a maximum for the number of sessions is good practice. Restricting the number of concurrent sessions will make sure accounts can no longer be shared between multiple or too many users. For a security reasons, application should likely log out the user from the initial session, that if a user tries to log in a second time he or she forgot to log out the first time or at least after changing the password.

Impact

An obvious mistake a user can make is forgetting to log out on a public computer. This alone is enough reason to invalidate a user session after a certain time, e.g. fifteen minutes. Another reason is that this also limits possibilities for smart hackers: especially in combination with other attacks like CSRF or click-jacking, session hijacking is a big risk. Initial tests revealed the session was active for around 20mins and concurrent sessions do not log out even after changing the password in one of the active sessions.

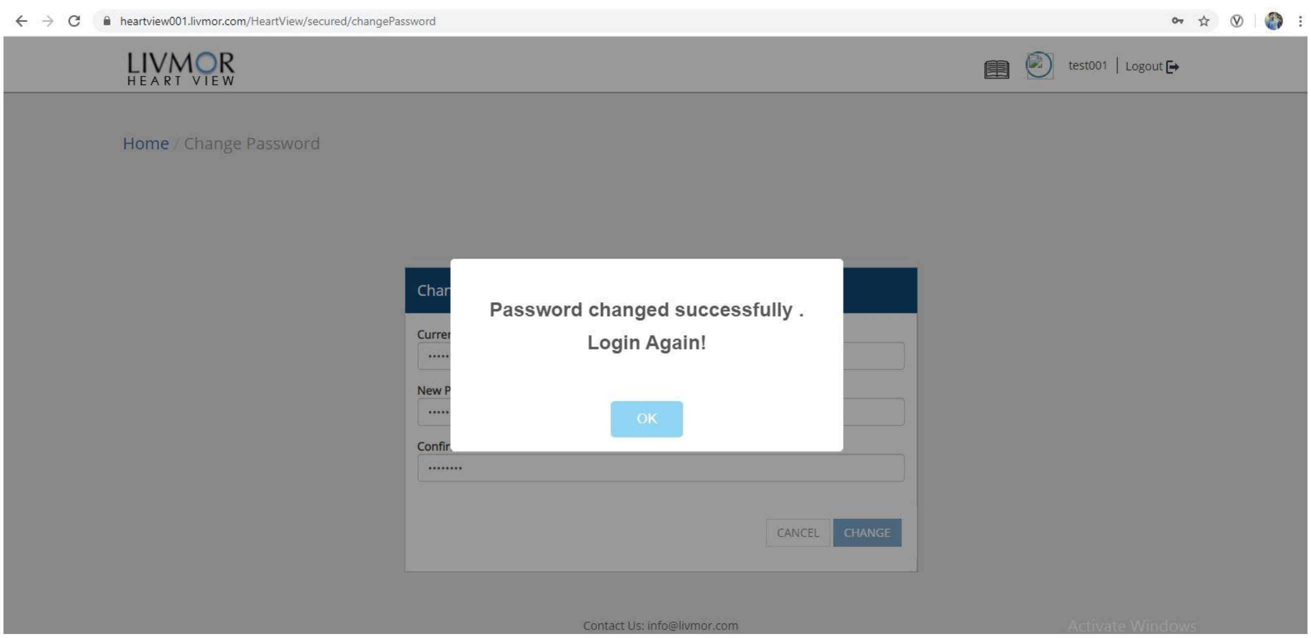
Remediation

It is recommended for web applications to add user capabilities that allow checking the details of active sessions at any time, monitor and alert the user about concurrent logons, provide user features to remotely terminate sessions manually, and track account activity history (logbook) by recording multiple client details such as IP address, User-Agent, login date and time, idle time, etc.

How to reproduce the Security defect

1. Login as any user (test case used test001/patient).
2. Do a concurrent login as test001 from a different system.
3. In the first login change password of the user, while application redirects to login page.
4. The concurrent session remains active and can perform transactions

Evidence



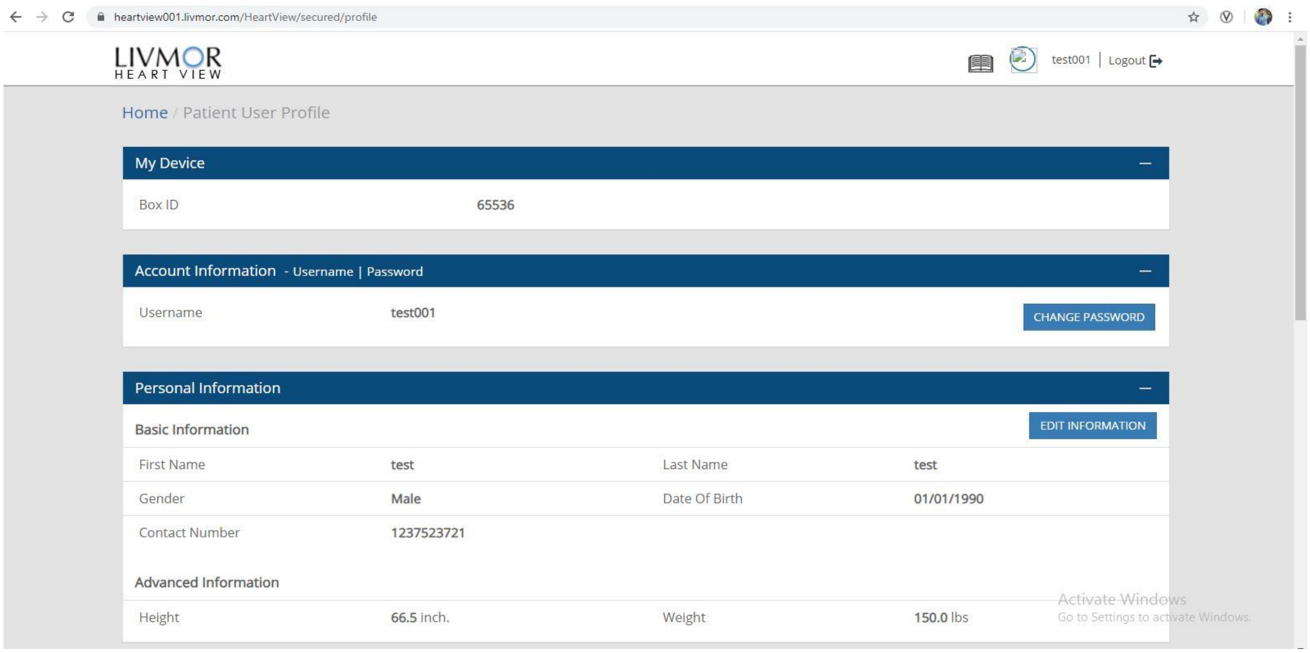
heartview001.livmor.com/HeartView/secured/changePassword

Home / Change Password

Password changed successfully .
Login Again!

Contact Us: info@livmor.com

Password changed successfully in Second concurrent session



heartview001.livmor.com/HeartView/secured/profile

Home / Patient User Profile

My Device

Box ID	65536

Account Information - Username | Password

Username	test001

Personal Information

Basic Information

First Name	test	Last Name	test
Gender	Male	Date Of Birth	01/01/1990
Contact Number	1237523721		

Advanced Information

Height	66.5 inch.	Weight	150.0 lbs

First session still found to be active

3.2 Directory Traversal

Name	Application exposes Apache Home page	**Impact**	Medium	**Risk Rating**	Medium
Ease of Exploit	Difficult	**Ease of Exploit**	Medium		
Category	Missing Functional Level Access Control				
URL / Impacted System	https://heartview001.livmor.com/HeartView/				

Description

Directory traversal attacks exploits bugs in the web server to gain unauthorized access to files and folders that are not in the public domain. Once the attacker has gained access, they can download sensitive information, execute commands on the server or install malicious software.

Impact

An organization's reputation can be ruined if the attacker edits the website content and includes malicious information or links to attacker's malformed website. The web server can be used to install malicious software on users who visit the compromised website. The malicious software downloaded onto the visitor's computer can be a virus, Trojan or Botnet Software, etc. Compromised user data may be used for fraudulent activities which may lead to business loss or lawsuits from the users who entrusted their details with the organization. As this web application is hosted on a staging server, this vulnerability is rated to be Medium. This vulnerability would be of a high risk on a production server or environment.

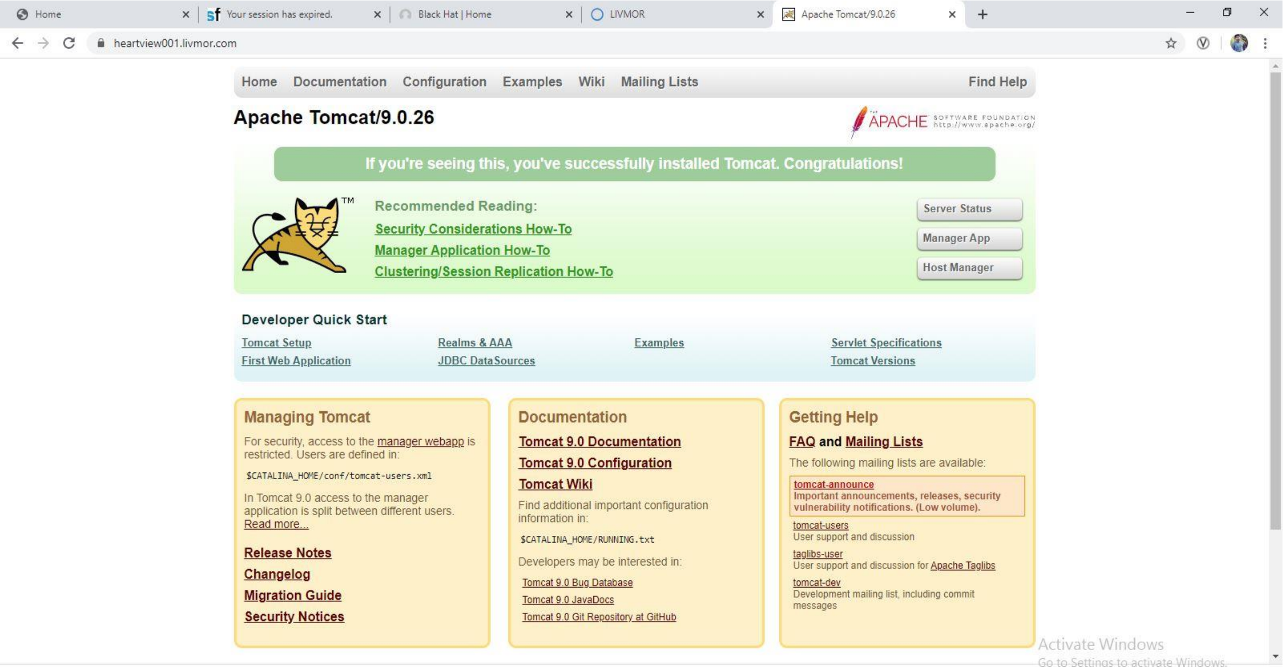
Remediation

Users should not be given access to unauthorized content of the server. In this case users should only be able to access the application content - https://halo.livmor.com/HeartView

How to reproduce the Security defect

1. Enter https://heartview001.livmor.com/HeartView/patient in the browser.
2. Change the URL to https://heartview001.livmor.com/

Evidence



Apache Tomcat/9.0.26

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To

Developer Quick Start

Tomcat Setup	Realms & AAA	Examples	Servlet Specifications
First Web Application	JDBC DataSources		Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. Read more...

Release Notes
Changelog
Migration Guide
Security Notices

Documentation

Tomcat 9.0 Documentation
Tomcat 9.0 Configuration
Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

Tomcat 9.0 Bug Database
Tomcat 9.0 JavaDocs
Tomcat 9.0 Git Repository at GitHub

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

3.3 Click-Jacking

Name	Frame able Response, X-Frame-Options header missing	**Impact**	Medium	**Risk Rating**	Medium
Ease of Exploit	Easy	**Likelihood**	Medium		
Category	Phishing/Social Engineering Attacks				
URL / Impacted System	https://heartview001.livmor.com/HeartView/				

Description

Clickjacking is a malicious technique that consists of deceiving a web user into interacting by clicking with something different to what the user believes they are interacting with. This type of attack, that can be used alone or in combination with other attacks, could potentially send unauthorized commands or reveal confidential information while the victim is interacting with seemingly harmless web pages. Application has many instances where pages are missing X-frame headers to avoid clickjacking.

Impact

Attacker loads frame with high opacity onto the victim user's application page, something which is not the same what the user believed to be interacting with. Proof of clickjacking instance recorded is attached in the Evidence.

Remediation

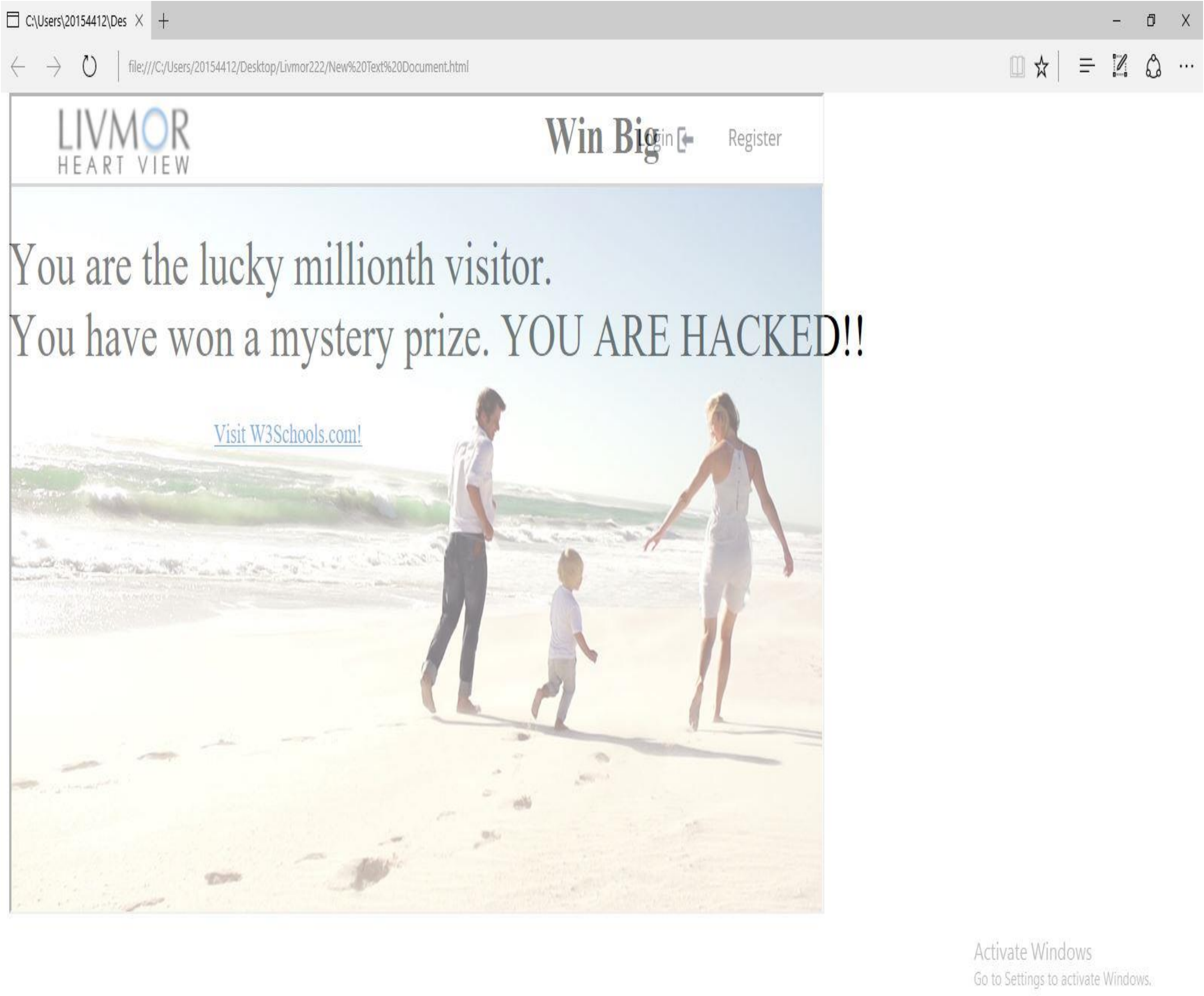
The **X-Frame-Options** HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe> or <object>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

How to reproduce the Security defect

1. Write the following code into a notepad and save it as dellclickjacking.html (in our case on desktop)

```
<html>
<h1 style="text-align:center">Win Big</h1>
   <p style="font-size: 38px;">You are the lucky millionth visitor.<br>You have won
     a mystery prize. YOU ARE HACKED!!</p>
   <div style="z-index:10; opacity:0.5; position:absolute; top:0px; ">
   <iframe scrolling="no" style="width:800px; height:500px;"
     src="https://halo.livmor.com/HeartView/"> </iframe>
   </div>
   <div style="position:absolute; top:200px; left:210px;">
    <a href="https://www.google.com">Visit W3Schools.com!</a>
   </div>
  </html>
```

Evidence



file:///C:/Users/20154412/Desktop/Livmor222/New%20Text%20Document.html

You are the lucky millionth visitor.
You have won a mystery prize. YOU ARE HACKED!!

3.4 No Account Lockout

Name	Account lock out mechanism is not implemented for physician Account	**Impact**	Medium	**Risk Rating**	Medium
Ease of Exploit	Automated Tools Available	**Likelihood**	Medium		
Category	Authentication				
URL / Impacted System	https://heartview001.livmor.com/HeartView/				

Description

Account lockout mechanisms are used to mitigate brute force password guessing attacks. Accounts are typically locked after 3 to 5 unsuccessful login attempts and can only be unlocked after a predetermined period, via a self-service unlock mechanism, or intervention by an administrator.

Impact

An Intruder may gain access as legitimate user through brute forcing the weak username and password implemented in the application. This would have impact on the whole application if attacker gains superuser access to the application. The password complexity check is not performed at the server side for the registration/change password function.

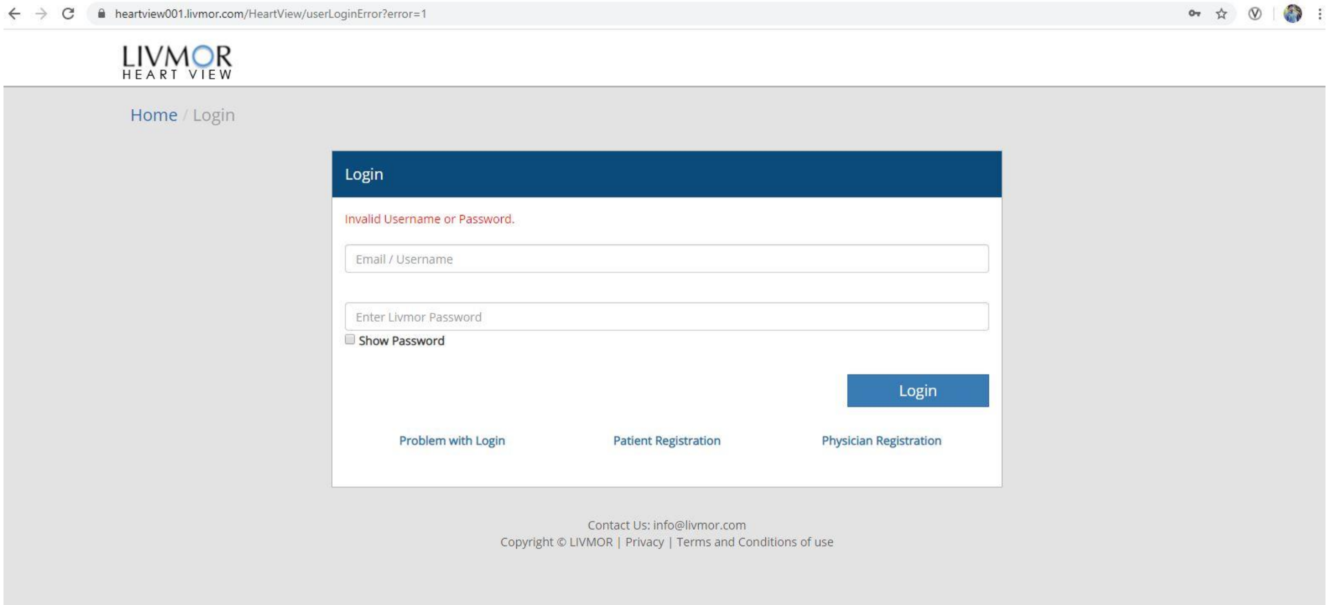
Remediation

The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator. A CAPTCHA may hinder brute force attacks, but CAPTCHA should be perceived as a rate limiting protection only which stops the attacker for a limited amount of time, also can use alternative verification channels like SMS authentication, OTP tokens etc.

How to reproduce the Security defect

1. 1. Browse to https://heartview001.livmor.com/HeartView/userLogin
2. 2. Provide invalid password for ‘test.phy@livmor.com (physician account)’ user for 5 times.
3. 3. Application Logs in upon providing valid credentials the 6th time.

Evidence



heartview001.livmor.com/HeartView/userLoginError?error=1

Home / Login

Login

Invalid Username or Password.

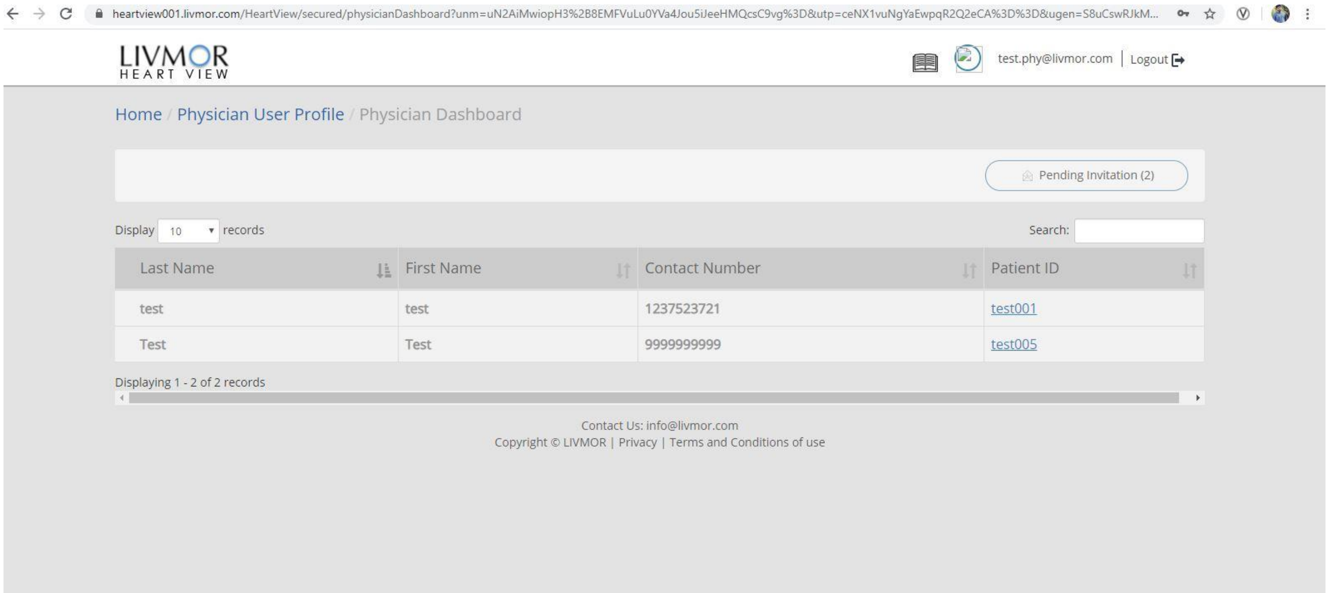
Email / Username

Enter Livmor Password

□ Show Password

Contact Us: info@livmor.com
Copyright © LIVMOR | Privacy | Terms and Conditions of use

Able to successfully login after 5 failed login attempts



heartview001.livmor.com/HeartView/secured/physicianDashboard?unm=uN2AiMwiopH3%2B8EMFVuLu0YVa4Jou5iJeeHMQcsC9vg%3D&utp=ceNX1vuNgYaEwpqR2Q2eCA%3D%3D&ugen=S8uCswRJkM...

test.phy@livmor.com | Logout

Home / Physician User Profile / Physician Dashboard

Display 10 records

Search:

Last Name	First Name	Contact Number	Patient ID
test	test	1237523721	test001
Test	Test	9999999999	test005

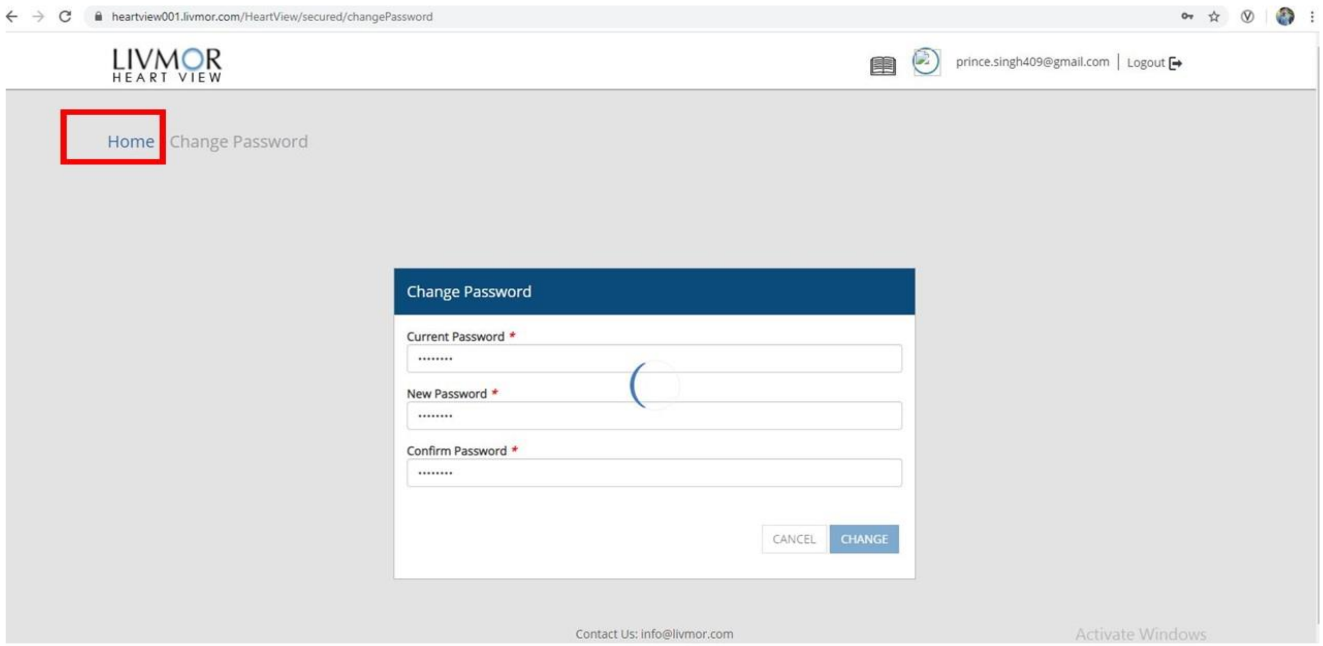
Displaying 1 - 2 of 2 records

Contact Us: info@livmor.com
Copyright © LIVMOR | Privacy | Terms and Conditions of use

3.5 No Session Logout

Name	Account log out mechanism is not implemented for physician Account as well as the patient account after change password.	**Impact**	Medium	**Risk Rating**	Medium
Ease of Exploit	Automated Tools Available	**Likelihood**	Medium		
Category	Authentication				
URL / Impacted System	https://heartview001.livmor.com/HeartView/				
Description					
Account logout mechanisms are used to logout from the active sessions in the current system as well as the other systems as soon as the password changes. Every request from the session should be validated for the token and should be redirected to the login page after change password functionality is implemented.					
Impact					
An attacker may gain access to the session if the user forgets to close the screen after changing the password in a public system. The current active session can be used by the attacker to manipulate the user data/password again without the knowledge of the user.					
Remediation					
The most obvious way is logout all the current sessions and redirect to the login page on receiving any request from the active session after the user change the password.					
How to reproduce the Security defect					
1. Browse to https://heartview001.livmor.com/HeartView/secured/changePassword 2. Change the password. 3. Click on Home. It redirects to the current active session.					
Evidence					

After changing the password successfully. Click the Home button after changing the password.



heartview001.livmor.com/HeartView/secured/changePassword

prince.singh409@gmail.com | Logout

Home Change Password

Change Password

Current Password *

••••••••

New Password *

••••••••

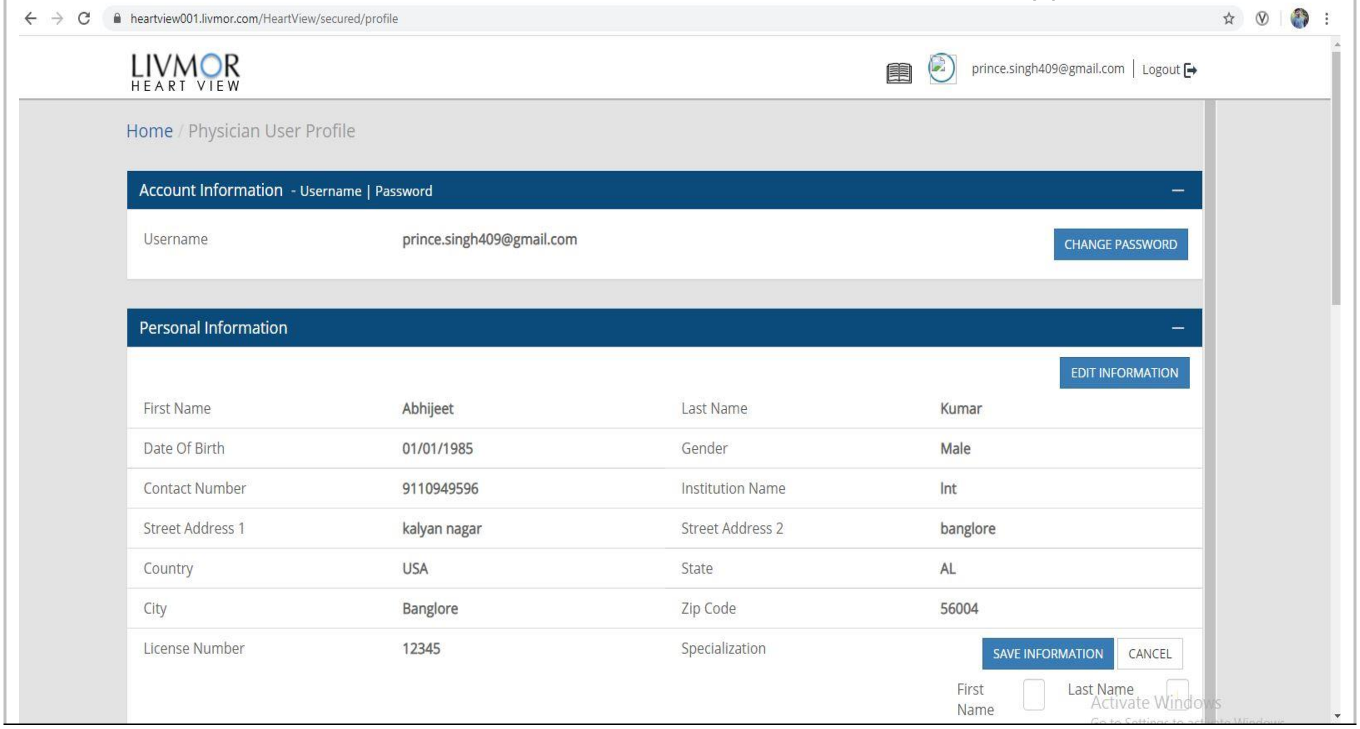
Confirm Password *

••••••••

CANCEL CHANGE

Contact Us: info@livmor.com

Able to remain active at the current session and able to view and modify profile data.



heartview001.livmor.com/HeartView/secured/profile

prince.singh409@gmail.com | Logout

Home / Physician User Profile

Account Information - Username | Password

Username prince.singh409@gmail.com CHANGE PASSWORD

Personal Information

EDIT INFORMATION

First Name	Abhijeet	Last Name	Kumar
Date Of Birth	01/01/1985	Gender	Male
Contact Number	9110949596	Institution Name	lnt
Street Address 1	kalyan nagar	Street Address 2	banglore
Country	USA	State	AL
City	Banglore	Zip Code	56004
License Number	12345	Specialization	

SAVE INFORMATION CANCEL

First Name □ Last Name □

3.6 Server side Password Complexity Check

Name	Password complexity is not validated at server side	**Impact**	Low	**Risk Rating**	Low
Ease of Exploit	Easy	**Likelihood**	Medium		
Category	Input Validation				
URL / Impacted System	https://heartview001.livmor.com/HeartView				

Description

The password complexity check for the all user while registering/changing password is only performed at the browser side but not on the server side, by tampering the parameters through intercepting the request can bypass the complexity requirements and set any password of user’s own choice. User with penetration skills can bypass password complexity requirements.

Impact

With no account lock out mechanism implemented in the application, bypassing the password complexity requirements and using weak passwords for accounts may lead to brute force attacks and gain unauthorized access to the application.

Remediation

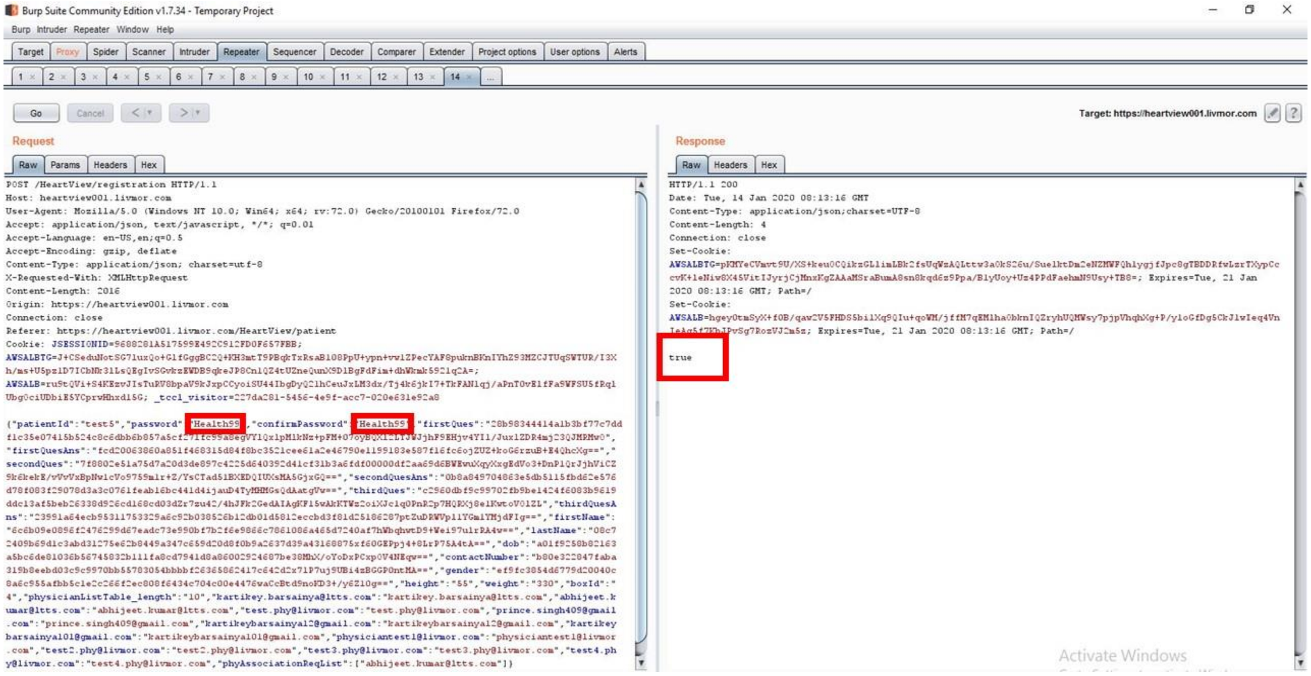
Security controls for strong password complexity should be enforced on client side and server side also.

How to reproduce the security defect

1. Register as new patient through - https://heartview001.livmor.com/HeartView/patient
2. Enter password as expected by the application (min 8 characters)
3. Intercept the request in BURP proxy
4. Change the password values as desired
5. Release the request and observe the response

Evidence

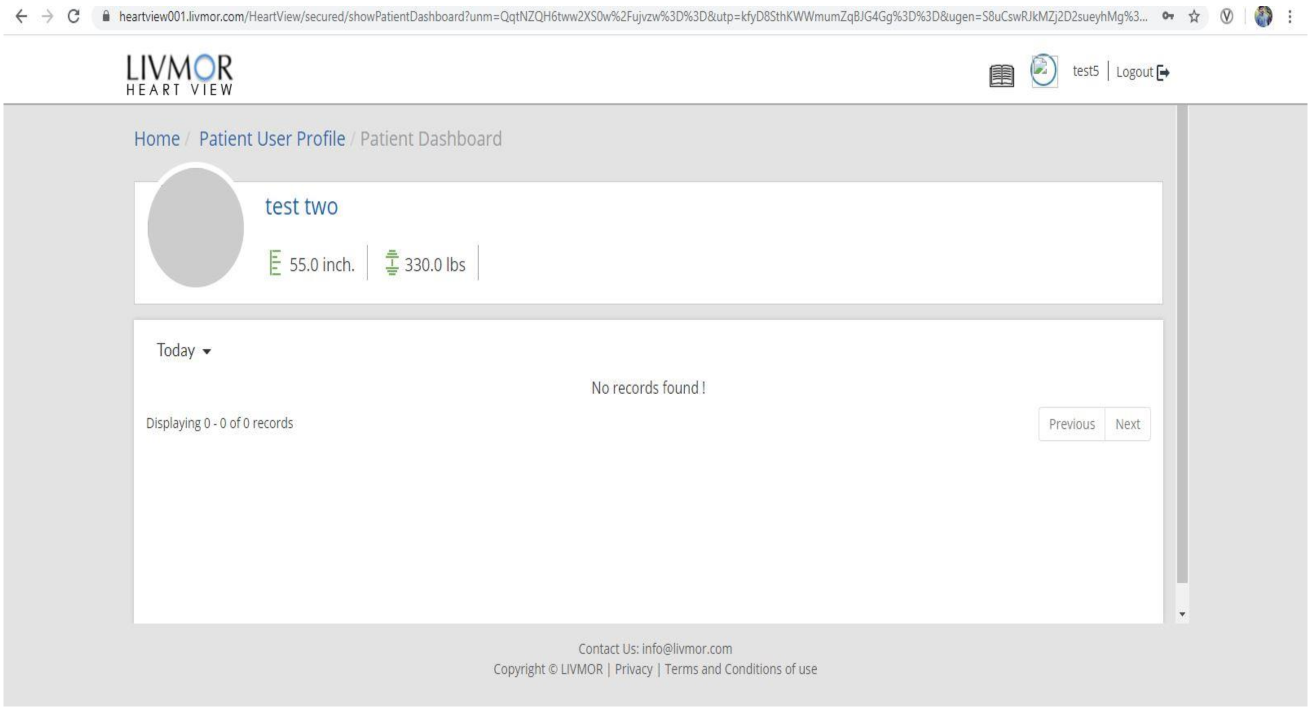
Alter the password field after capturing request at the time of registration.


Burp Suite Community Edition v1.7.34 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × 10 × 11 × 12 × 13 × 14 × ...
Go Cancel < >
Target: https://heartview001.livmor.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Activate Windows

```
POST /HeartView/registration HTTP/1.1
Host: heartview001.livmor.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 2016
Origin: https://heartview001.livmor.com
Connection: close
Referer: https://heartview001.livmor.com/HeartView/patient
Cookie: JSESSIONID=9688281A517599E492C912FD0F657FBB;
AWSALBTG=J+CSeduNotSG7luxQo+GlfGggBC2Q+KH3mtT9PBqkTxRsaB108PpU+ypn+vwlZPecYAF8puknBKnIYhZ93MZCJTUqSWTUR/I3X
h/ms+U5pz1D7ICbNk31LsQEgIvSGvkzEWDB9qkeJP8Cn1QZ4tUZneQunX9DlBgFdFim+dhWkmk5921q2A=;
AWSALB=ru9tQVi+S4KEzvJIsTuRV8bpaV9kJxpCCyoiSU44IbgDyQ21hCeuJxLM3dx/Tj4k6jkI7+TkFANlqj/aPnT0vElfFa9WFSU5fRql
Ubg0ciUDbiE5YCprwHhxdl5G; _tccl_visitor=227da281-5456-4e9f-acc7-020e631e92a8

{"patientId":"test5","password":"Health99","confirmPassword":"Health99","firstQues":"28b98344414a1b3bf77c7dd
f1c35e07415b524c8c6dbb6b857a5cf271fc99a8egVY1QxlpMlkNz+pFM+07oyBQX12LTJWJjhF9EHjv4YI1/Jux1ZDR4mj23QJMRMw0",
"firstQuesAns":"fcd20063860a851f468315d84f8bc3521cee61a2e46790e1199183e587f16fc6ojZUZ+koG6rzuB+E4QhcXg==","
secondQues":"7f8802e51a75d7a20d3de897c4225d640392d41cf31b3a6fdf00000df2aa69d6BWEwuXqyXxgEdVo3+DnP1QrJjhViCZ
9k6kekE/vVvVxBpNwlcVo9759mlr+Z/YsCTad51BXEDQIUXsMA5GjxGQ==","secondQuesAns":"0b8a849704863e5db5115fbd62e576
d78f083f29078d3a3c0761feab16bc441d4ijauD4TyMHMGsQdAatgVw==","thirdQues":"c2960dbf9c99702fb9be1424f6083b9619
ddc13af5beb26338d926cd168cd03dZr7zu42/4hJFk2GedAIAgKF15wAkKTWz2oiXJc1q0PnR2p7HQRXj8elKwtoV01ZL","thirdQuesA
ns":"23991a64ecb95311753329a6c92b038526b12db01d5812eccbd3f81d25186287ptZuDRWVp11YGm1YMjdFIg==","firstName":
"6c6b09e0896f2476299d67eadc73e990bf7b2f6e9866c7861086a465d7240af7hWbqhwtD9+Wei97ulrRA4w==","lastName":"08c7
2409b69d1c3abd31275e62b8449a347c659d20d8f0b9a2637d39a43168875xf60GEPpj4+8LrP75A4tA==","dob":"a01f9258b82163
a5bc6de81036b56745832b111fa8cd7941d8a86002924687be38MhX/oYoDxPCxp0V4NEqw==","contactNumber":"b80e322847faba
319b8eebd03c9c9970bb55783054bbbbf26365862417c642d2x71P7uj9UBi4zBGGP0ntMA==","gender":"ef9fc3854d6779d20040c
8a6c955afbb5c1e2c266f2ec808f6434c704c00e4476waCcBtd9noKD3+/y6Z10g==","height":"55","weight":"330","boxId":"
4","physicianListTable_length":"10","kartikey.barsainya@ltts.com":"kartikey.barsainya@ltts.com","abhijeet.k
umar@ltts.com":"abhijeet.kumar@ltts.com","test.phy@livmor.com":"test.phy@livmor.com","prince.singh409@gmail
.com":"prince.singh409@gmail.com","kartikeybarsainya12@gmail.com":"kartikeybarsainya12@gmail.com","kartikey
barsainya101@gmail.com":"kartikeybarsainya101@gmail.com","physiciantest1@livmor.com":"physiciantest1@livmor
.com","test2.phy@livmor.com":"test2.phy@livmor.com","test3.phy@livmor.com":"test3.phy@livmor.com","test4.ph
y@livmor.com":"test4.phy@livmor.com","phyAssociationReqList":["abhijeet.kumar@ltts.com"]}
```

```
HTTP/1.1 200
Date: Tue, 14 Jan 2020 08:13:16 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 4
Connection: close
Set-Cookie:
AWSALBTG=pKMYeCVmvt9U/XS+keu0CQikzGLlimLBk2fsUqWzAQLttw3a0kS26u/SuelktDm2eNZMWFQhlygjfJpc8gTBDDRfwLzrTXypCc
cvK+leNiw8X45VitIJyrjCjMnxKgZAAaMSraBumA8sn8kqd6z9Ppa/BlyUoy+Uz4PPdFaehmN9Usy+TB8=; Expires=Tue, 21 Jan
2020 08:13:16 GMT; Path=/
Set-Cookie:
AWSALB=hgeyOtmSyX+f0B/qaw2V5FHDS5bilXq9QIu+qoWM/jffM7qEMlha0bknIQZryhUQMWsy7pjpVhqhXg+P/yloGfDg5CkJlwIeq4Vn
IeAg5f7KhJPvSg7RozVJ2m5z; Expires=Tue, 21 Jan 2020 08:13:16 GMT; Path=/

true
```

Password is changed and able to login successfully.


heartview001.livmor.com/HeartView/secured/showPatientDashboard?unm=QqtNZQH6tww2XS0w%2Fujvzw%3D%3D&utp=kfyD8SthKWWmumZqBJG4Gg%3D%3D&ugen=S8uCswRJkMZj2D2sueyhMg%3...
LIVMOR
HEART VIEW
test5 | Logout
Home / Patient User Profile / Patient Dashboard
test two
55.0 inch.
330.0 lbs
Today
No records found !
Displaying 0 - 0 of 0 records
Previous
Next
Contact Us: info@livmor.com
Copyright © LIVMOR | Privacy | Terms and Conditions of use

3.7 Insecure Password Creation

Name	Insecure Password Implementation	**Impact**	Low	**Risk Rating**	Low
Ease of Exploit	Easy	**Likelihood**	Medium		
Category	Information Leakage				
URL / Impacted System	https://heartview001.livmor.com/HeartView				

Description

Password Creation must contain special character as it makes the attacker difficult to brute force the password.

Impact

Without the special characters in the password, it will make the attacker easy to brute force the password.

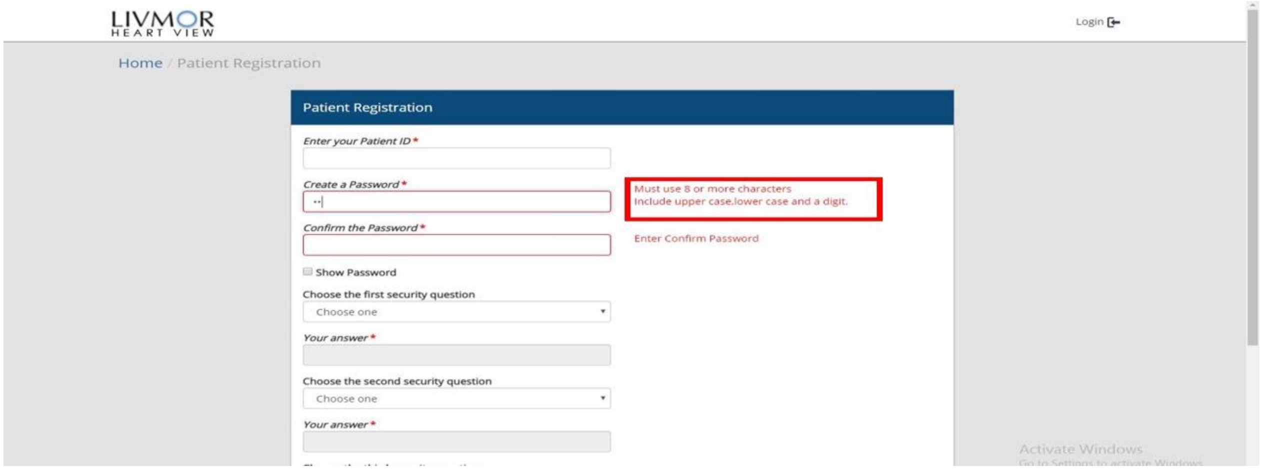
Remediation

Ensure that there must be a special character in the password when a user (patient/physician) registers to the application.

How to reproduce the security defect

1. Access the LIVMOR Web Application
2. Visit 'Register' page
3. Register the password

Evidence



Enter your Patient ID *

Create a Password * ••

Must use 8 or more characters
Include upper case,lower case and a digit.

Confirm the Password *

Enter Confirm Password

Choose the first security question

Your answer *

Choose the second security question

Your answer *

4. Abbreviation

ARP	Address Resolution Protocol
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CSRF	Cross Site Request Forgery
HTML	Hyper Text Markup Language
HTTP(S)	Hypertext transfer protocol (Secured)
ID	Identity Document
IE	Internet Explorer
IP	Internet Protocol
L&TTS	Larsen & Toubro Technology Services
MITM	Man In The Middle Attack
OTP	One Time Password
PII	Personal Identifiable Information
POC	Proof Of Concept
OWASP	Open Web Application Security Project
SIEM	Security Information and Event Management
SMS	Short Message Service
SQL	Structured Query Language
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VAPT	Vulnerability Assessment and Penetration testing
XSS	Cross Site Scripting

5. Appendix

zap1.html